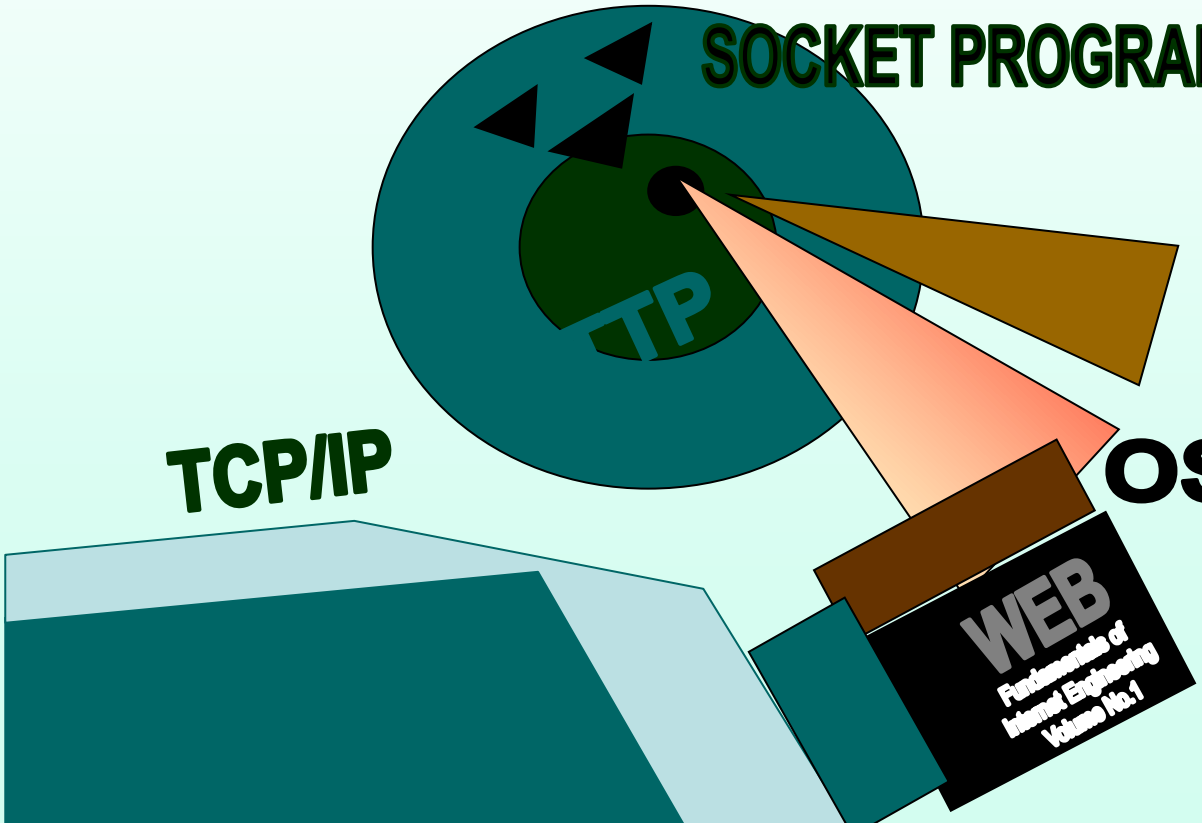
اصول مهندسي

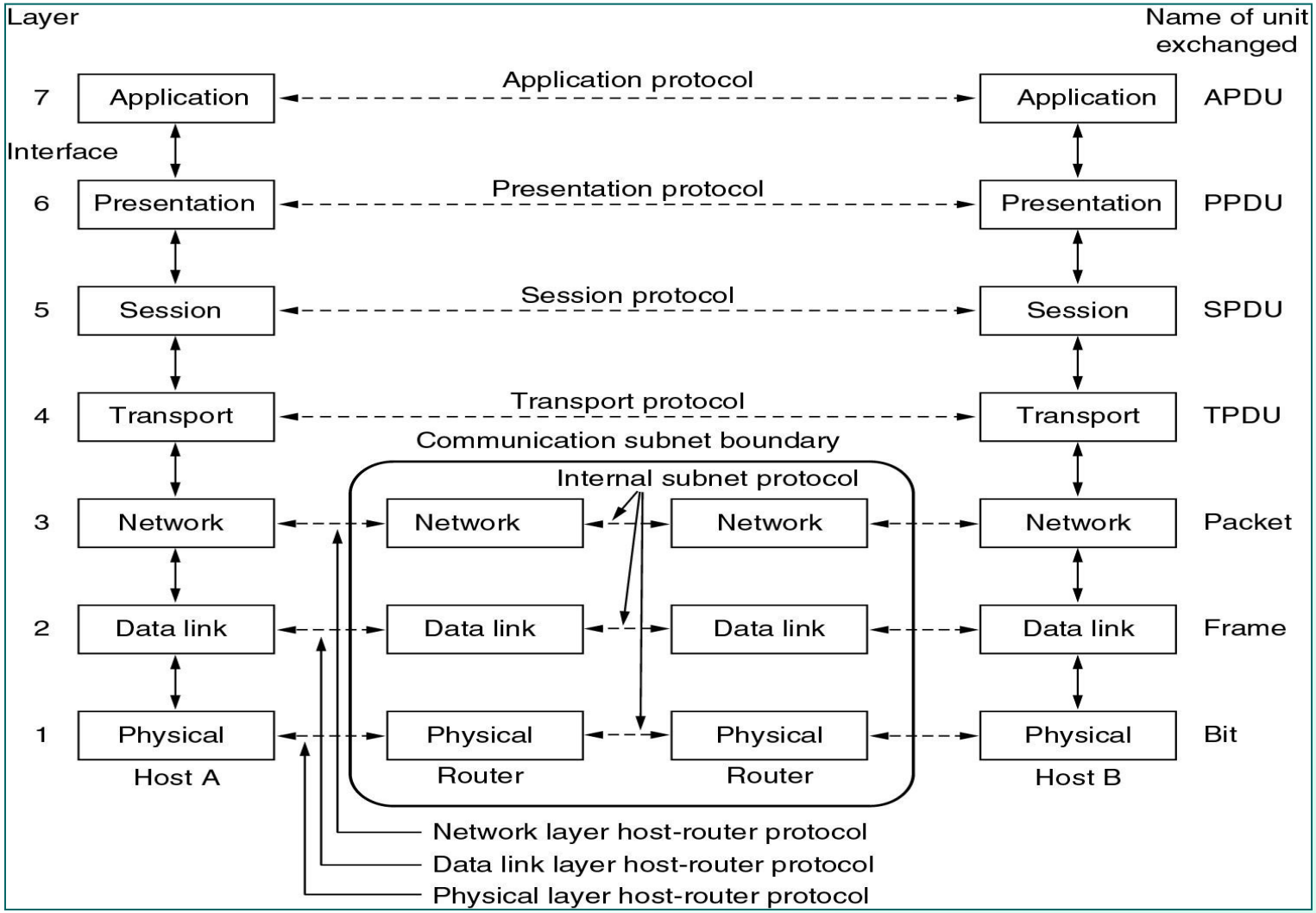
اينترنت



HTTP

HTTP

مدل هفت لايه‌اي OSI



لايه فيزيكي Physical Layer

- انتقال بيتها به صورت سيگنال الكتريكي و ارسال آن بر روي كانال
- واحد اطلاعات : بيت

پارامترهاي قابل توجه :

- ظرفيت كانال فيزيكي و نرخ ارسال
- نوع مدولاسيون
- چگونگي كوپلاژ با خط انتقال
- مسائل مكانيكي و الكتريكي مانند نوع كابل ، باند فركانسي ، نوع رابط (كانكتور) كابل

لايه پيوند داده - Data Link Layer

وظايف :

- به مقصد رساندن داده‌ها روي يك كانال انتقال بدون خطا و مطمئن با استفاده از مكانيزمهاي كشف و كنترل خطا.
- شكستن اطلاعات ارسالي از لايه بالاتر به واحدهاي استاندارد و كوچكتر و مشخص نمودن ابتدا و انتهاي آن از طريق نشانه‌هاي خاصي بنام Delimiter.
- كشف خطا از طريق اضافه كردن بيتهاي كنترل خطا
- كنترل جريان يا تنظيم جريان ارسال فريمها (مكانيزمهاي هماهنگي بين مبدأ و مقصد)
- اعلام وصول يا عدم رسيدن داده‌ها به فرستنده
- وضع قراردادهائي براي جلوگيري از تصادم سيگنالهاي ارسالي (اين قراردادها در زيرلايه‌اي بنام MAS تعريف شده است)
- كنترل سخت‌افزار لايه فيزيكي

لايه شبكه

- سازماندهي اطلاعات بصورت بسته و ارسال جهت انتقال مطمئن به لايه پيوند داده‌ها
- تعيين مسير هر بسته ارسالي براي رسيدن به مقصد
- جلوگيري از ازدحام و ترافيك در بين مسيريابها و سوئيچها
- اختصاص آدرسهاي مشخص و استاندارد براي هر بستة آماده ارسال
- اين لايه بدون اتصال است.

لايه انتقال

- ارسال يك بسته ويژه قبل از ارسال بسته‌ها براي اطمينان از آمادگي گيرنده براي دريافت اطلاعات
- شماره‌گذاري بسته‌هاي ارسالي براي جلوگيري از گم‌شدن يا ارسال دوباره بسته‌ها
- حفظ ترتيب جريان بسته‌هاي ارسالي
- آدرس‌دهي پروسه‌هاي مختلفي كه روي يك ماشين واحد اجرا مي‌شوند.
- تقسيم پيامهاي بزرگ به بسته‌هاي اطلاعاتي كوچكتر
- بازسازي بسته‌هاي اطلاعاتي و تشكيل يك پيام كامل
- شماره‌گذاري بسته‌هاي كوچكتر جهت بازسازي
- تعيين و تبيين مكانيزم نامگذاري ايستگاههاي موجود در شبكه

لايه جلسه Session Layer

- برقراري و مديريت يك جلسه
- شناسائي طرفين
- مشخص نمودن اعتبار پيامها
- اتمام جلسه‌ها
- حسابداري مشتريها

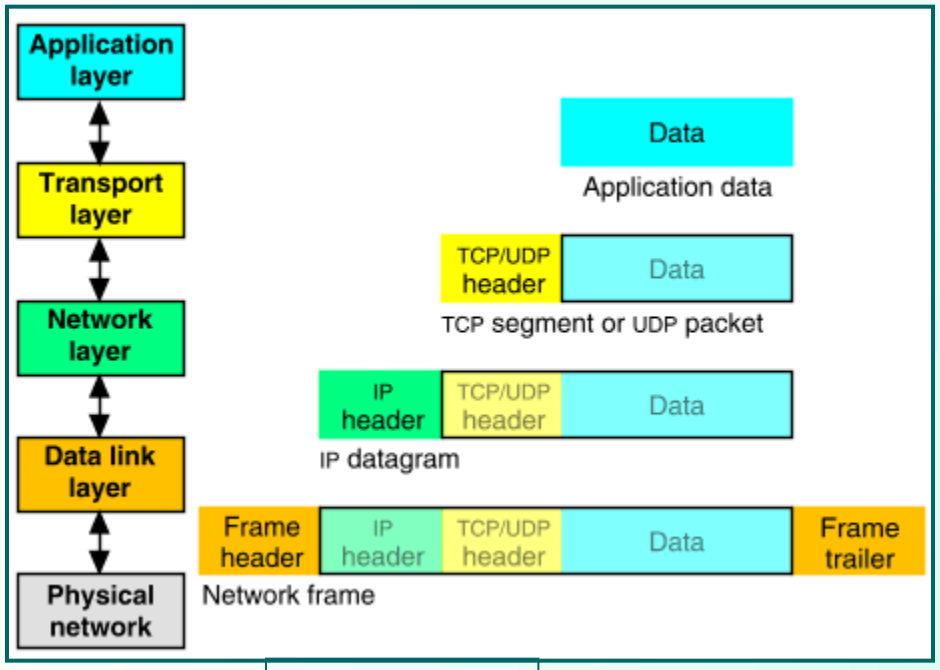
لايه ارائه (نمايش)

- فشرده‌سازي فايل
- رمزنگاري براي ارسال داده‌هاي محرمانه
- رمزگشائي
- تبديل كدها به يكديگر هنگام استفاده دو ماشين از استانداردهاي مختلفي براي متن

لايه كاربرد Application Layer

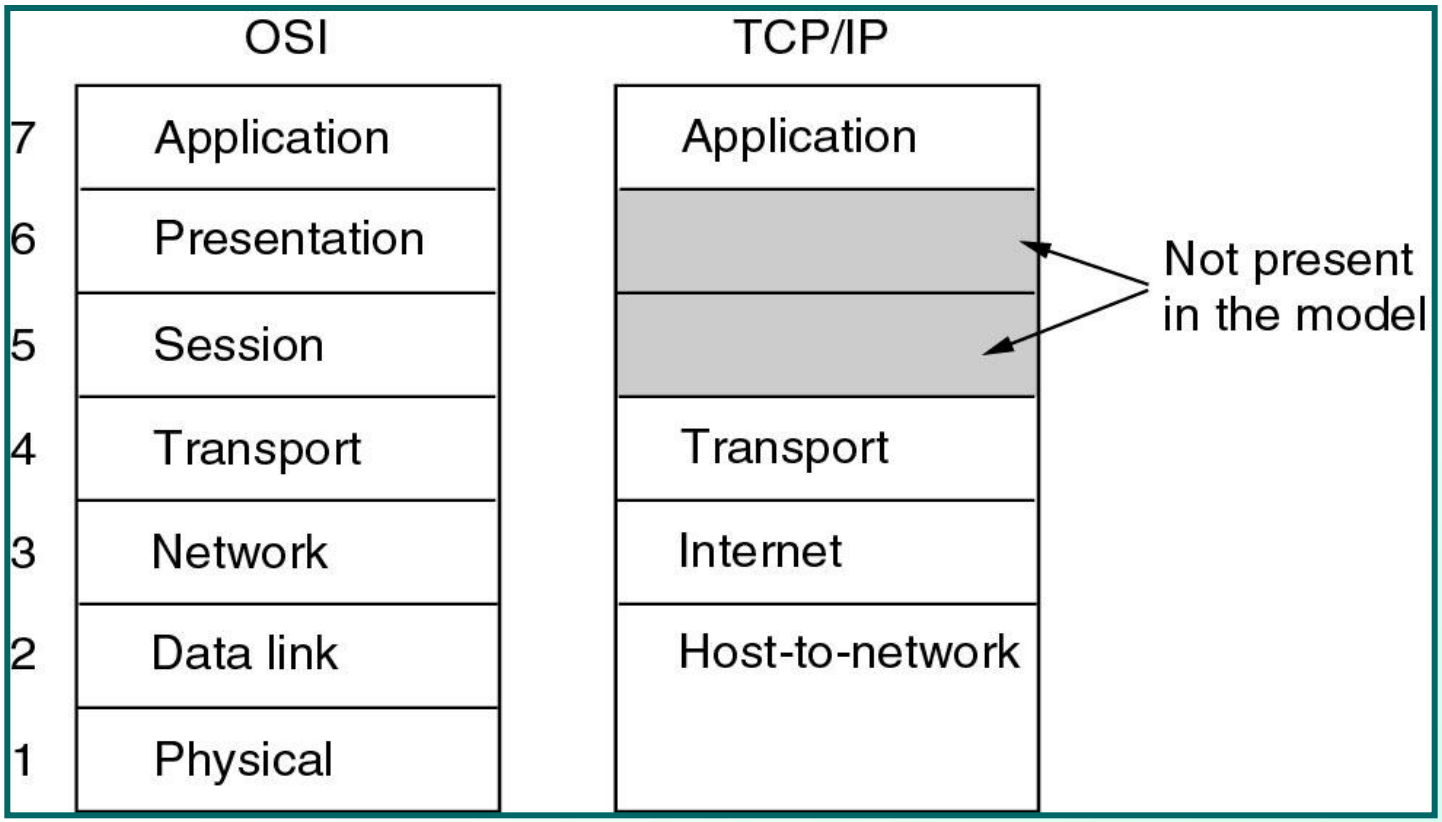
تعريف استانداردهائي نظير :

- انتقال نامه‌هاي الكترونيكي
- انتقال مطمئن فايل
- دسترسي به بانكهاي اطلاعاتي راه دور
- مديريت شبكه
- انتقال صفحه وب



مدل OSI

مدل چهارلايه‌اي TCP/IP



لايه‌هاي مدل TCP/IP

لايه‌ها	نامهاي معادل در برخي از كتب
لايه كاربرد Application layer	• لايه سرويسهاي كاربردي
لايه انتقال Transport layer	• لايه ارتباط ميزبان به ميزبان (Host to Host) • لايه ارتباط عناصر انتهائي (End to End Connection)
لايه شبكه Network layer	• لايه اينترنت • لايه ارتباطات اينترنت
لايه دسترسي به شبكه Network Interface	• لايه ميزبان به شبكه (Host to Network) • لايه رابط شبكه

لايه اول از مدل TCP/IP : لايه واسط شبكه

تعريف لايه‌هاي استاندارد سخت‌افزار ، نرم‌افزارهاي راه‌انداز و پروتكلهاي شبكه در اين لايه.

پروتكلهائي كه در لايه اول از مدل TCP/IP تعريف مي‌شوند ، مي‌توانند مبتني بر ارسال رشته بيت يا مبتني بر ارسال رشته بايت باشند.

لايه دوم از مدل TCP/IP : لايه شبكه

- بسته‌هاي IP بسته‌هاي اطلاعاتي در اين لايه
- هدايت بسته‌هاي IP روي شبكه از مبدأ تا مقصد كه اين عمل از نوع بدون اتصال مي‌باشد
- ويژگي ارسال چندپخشي يعني ارسال يك يا چند بسته اطلاعاتي به چندين مقصد گوناگون در قالب يك گروه سازماندهي‌شده
- پروتكلهائي كه در اين لايه استفاده مي‌شوند عبارتند از:

IP , IGMP , BOOTP , ARP , RARP , RIP , ICMP و ..

لايه سوم از مدل TCP/IP : لايه انتقال

برقراري ارتباط از طريق يك سرويس اتصال‌گرا و مطمئن با ماشينهاي انتهايي يا ميزبان.

ارسال و يا دريافت داده‌هاي تحويلي به اين لايه توسط برنامه‌هاي كاربردي و از طريق توابع سيستمي

لايه چهارم از مدل TCP/IP : لايه كاربرد

خدماتي كه در اين لايه صورت مي‌گيرد در قالب پروتكلهاي استاندارد زير
به كاربر ارائه مي‌شود :

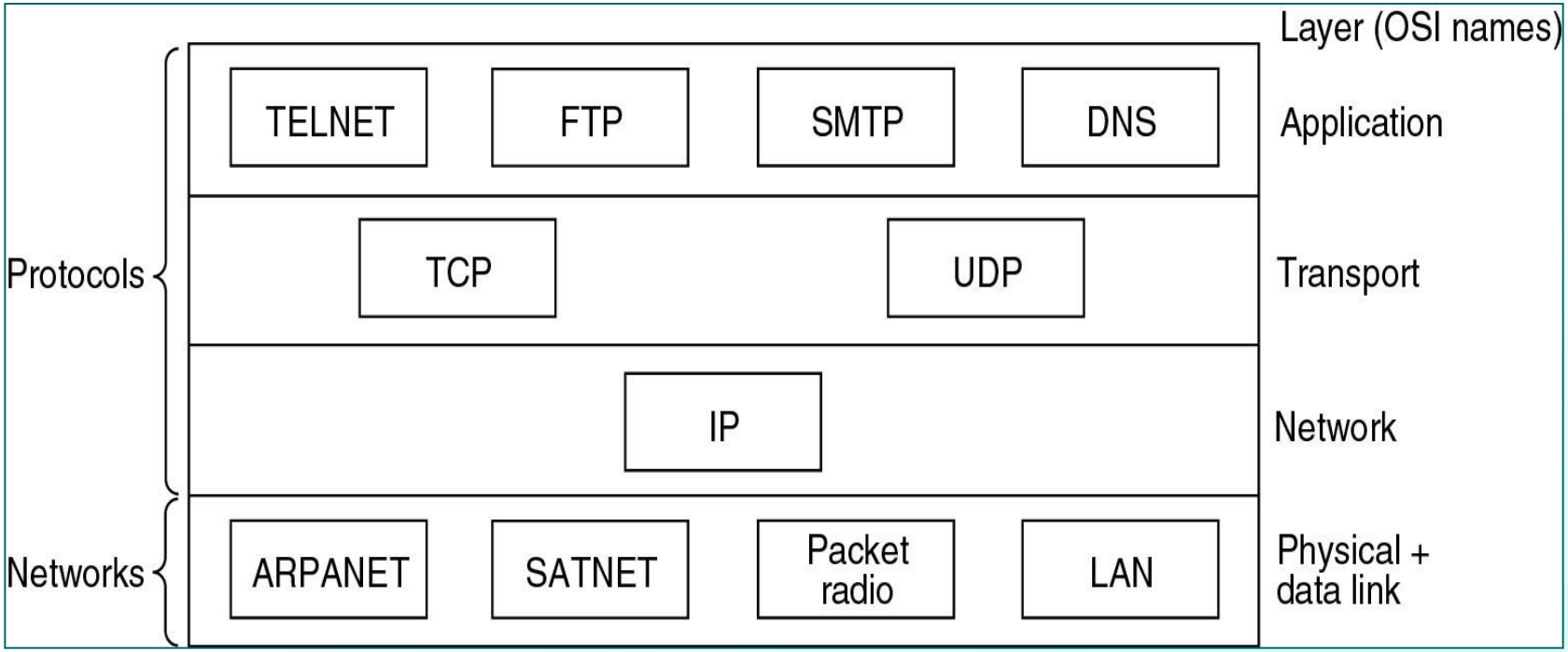
شبيه‌سازي ترمينال

انتقال فايل يا FTP

مديريت پست الكترونيكي

خدمات انتقال صفحات ابرمتني

پروتکلهاي رايج در لايه ها



فصل اول: لایه IP در شبکه اینترنت

هدفهای آموزشی :

- مفاهیم لایه IP
- تشریح پروتکل و بسته‌هاي IP
- آدرس‌دهي ماشینها و کلاسهاي آدرس
- الگوهاي زیر شبکه
- پروتکل ICMP
- پروتکلهاي BOOTP,RARP,ARP

لایه IP

هدایت بسته‌هاي اطلاعاتي از شبکه‌اي به شبکه‌هاي ديگر

آدرسهای MAC

- آدرسهاي قابل تعريف در لايه اول (لايه فيزيکي) جهت انتقال فريمها روي کانال
- وابسته به ساختار شبکه

در پروتکل CSMA/CD شبکه
MAC (Ethernet) آدرس = ۶ بایت

در پروتکل SLIP فیلد
آدرس MAC وجود **ندارد**

- بي‌نظمي در شبكه‌هاي مختلف
- تنوع توپولوژي و پروتكلها
- تفاوت در روشهاي آدرس‌دهي

- تعريف آدرسهاي جهاني و استاندارد براي تمامي ايستگاهها
- ساختار يكسان بسته قرارگرفته درون فيلد داده از فريم هر شبكه
- عدم وابستگي بسته به نوع شبكه و سخت افزار

بسته IP

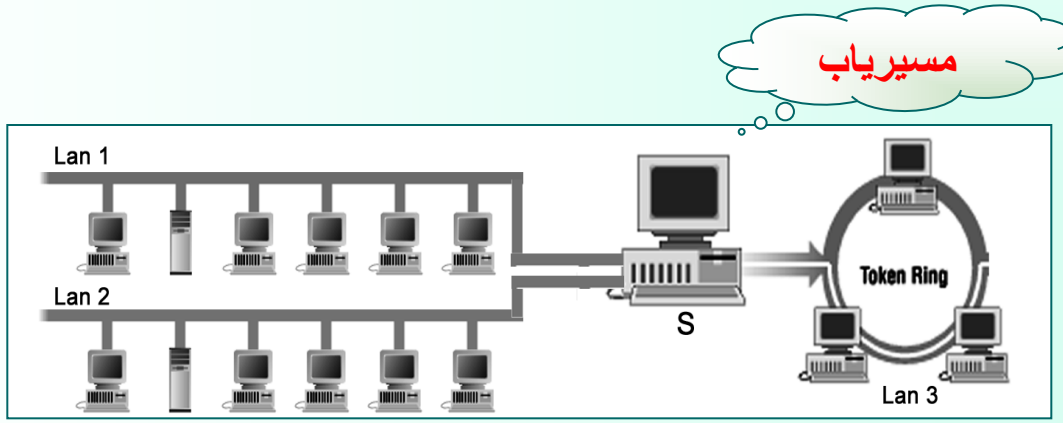
واحد اطلاعاتي كه درون فيلد داده از فريم فيزيكي قرار گرفته و با عبور از يک شبكه به شبكه ديگر تغيير نمي‌كند.

آدرس IP

آدرس جهاني و مشخص كننده ماشين به صورت يكتا و فارغ از ساختار شبكه‌اي

مسيرياب (Router)

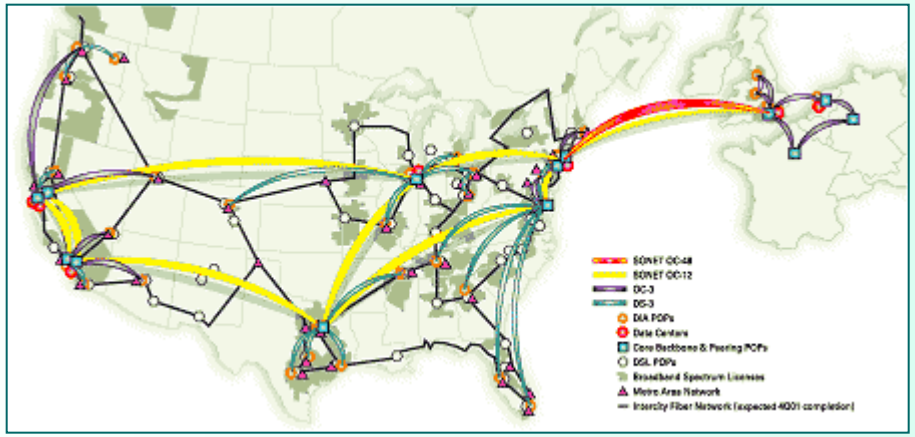
- ماشيني با تعدادي ورودي و خروجي
- دريافت بسته‌هاي اطلاعاتي از ورودي و هدايت و انتخاب كانال خروجي مناسب بر اساس آدرس مقصد



لایه اینترنت (Network)

زیرشبکه (Subnet) : زیر ساخت ارتباطي شبکه‌ها

ستون فقرات (Backbone) : خطوط ارتباطي با پهناي باند (نرخ ارسال) بسیار بالا و مسیریابهاي بسیار سریع و هوشمند در قسمت زیرشبکه



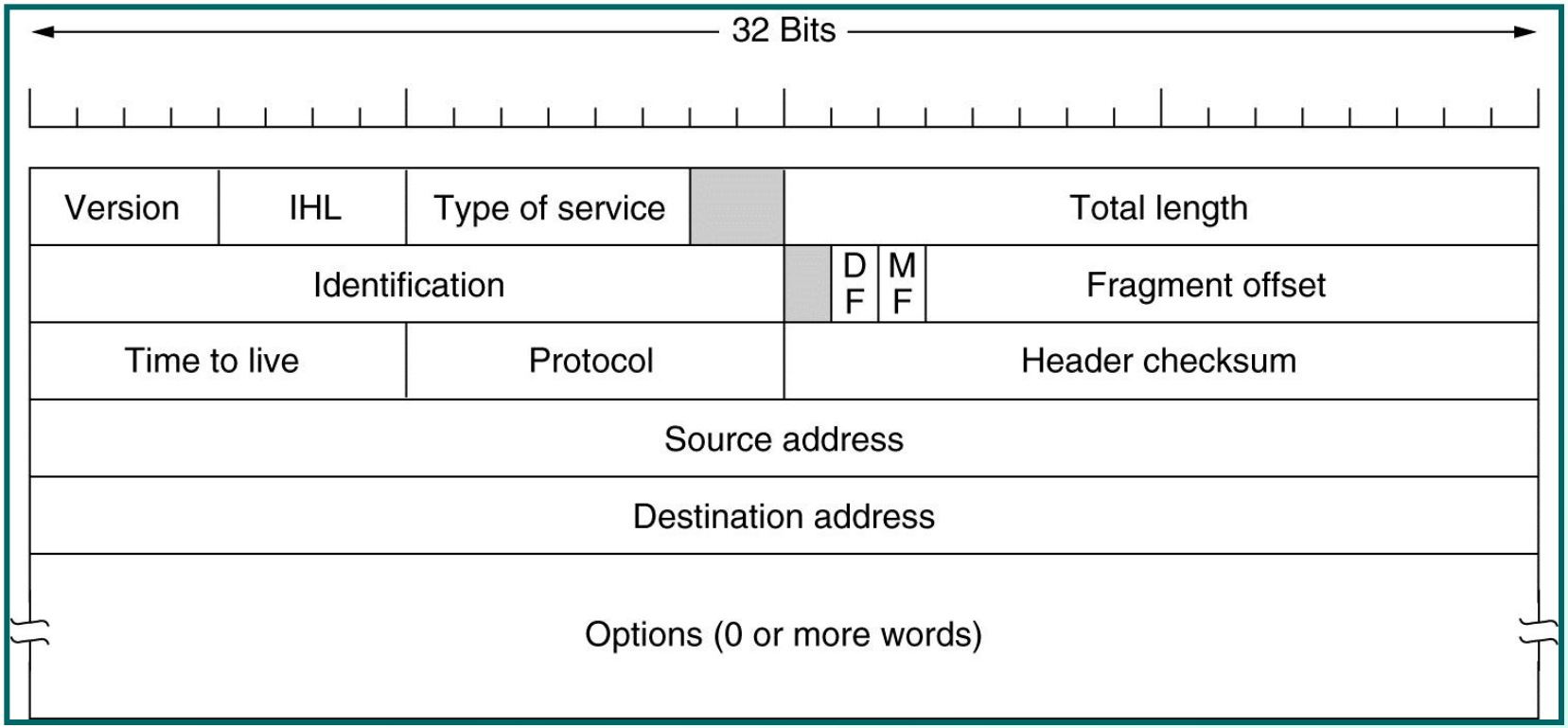
پروتكل IP:

- قرارداد حمل و تردد بسته‌هاي اطلاعاتي
- مديريت و سازماندهي مسيريابي صحيح بسته‌ها از مبدأ به مقصد

ديتاگرام

واحد اطلاعات كه به صورت يكجا از لايه IP به لايه انتقال تحويل داده مي‌شود يا بالعكس لايه انتقال آنرا جهت ارسال روي شبكه به لايه IP تحويل داده و ممكن است شكسته شود.

قالب بسته IP


32 Bits
Version
IHL
Type of service
Total length
Identification
D F
M F
Fragment offset
Time to live
Protocol
Header checksum
Source address
Destination address
Options (0 or more words)

فیلد Version

- چهار بیت
- مشخص کننده نسخه پروتکل IP

Version= 0100 نسخه شماره 4 پروتکل IP

نسخه شماره 6 پروتکل IP

فیلد IHL (IP Header Length)

- چهار بیتي
- مشخص کننده طول کل سرآیند بسته بر مبناي کلمات 32 بیتي
- حداقل مقدار فیلد IHP عدد 5

فیلد Type of sevice

- فیلد 8 بیتي
- مشخص کننده درخواست سرویس ویژه‌اي توسط ماشین میزبان از مجموعه زیرشبکه براي ارسال دیتاگرام

بخشهای فیلد:

تعیین کننده اولویت بسته IP

P2	P1	P0	D	T	R	-	-
تقدم بسته			تأخیر	توان خروجي	قابلیت اطمینان	بلااستفاده	

قراردادن عدد 1 توسط ماشین میزبان در این بیتها جهت انتخاب مسیر مناسب توسط مسیریابها

فیلد Total Length

- فیلد 16 بیتي
- مشخص کننده طول کل بسته IP (مجموع اندازه سرآیند و ناحیه داده)
- حداکثر طول کل بسته IP 65535 بایت

فیلد Identification

- فیلد 16 بیتي
- مشخص کننده شماره یک دیتاگرام واحد

فیلد Fragment Offset

الف) بیت DF (Don’t Fragment):

با یک شدن این بیت در یک بسته IP هیچ مسیریابي 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 بعدي از یک دیتاگرام

ج) Fragment offset

- 13 بیتي
- نشان دهنده شماره ترتیب هر قطعه ازیک دیتاگرام شکسته شده
- حداکثرتعداد قطعات یک دیتاگرام 8192

فیلد Time To Live

- فیلد 8 بیتي
- مشخص کننده طول عمر بسته IP
- حداکثر طول عمر بسته IP = 255

فیلد پروتکل

- نشان دهنده شماره پروتکل لایه بالاتر متقاضي ارسال دیتاگرام
- فیلد 8 بیتي

فيلد Header Ckecksum

- فيلد 16 بيتي
- كشف خطاهاي احتمالي در سرآيند هر بسته IP

روش محاسبه كد كشف خطا:

جمع كل سرآيند به صورت دو بايت دو بايت

حاصل جمع به روش مكمل يك منفي مي گردد

قرارگرفتن عدد منفي حاصله در فيلد Header Ckecksum

فیلد Source Address

- فیلد 32 بیتي
- مشخص کننده آدرس ماشین مبدأ

فیلد Destination Address

- فیلد 32 بیتي
- مشخص کننده آدرس IP ماشین مقصد

فیلد Payload

قرارگرفتن داده هاي دريافتي از لايه بالاتر دراين فيلد

فیلد اختیاری Option

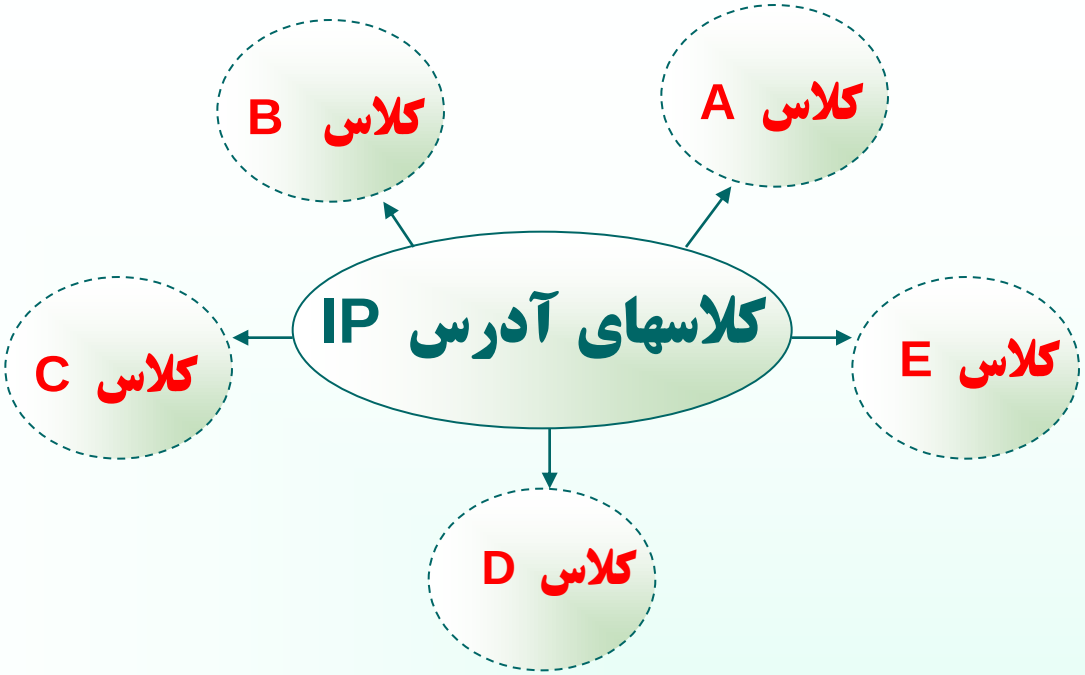
- حداکثر 40 بایت
- محتوي اطلاعات جهت يافتن مسير مناسب توسط مسيريابها

آدرسها در اينترنت و اينترانت

شناسايي تمام ابزار شبكه (ماشينهاي ميزبان, مسيريابها, چاپگرهاي شبكه) در اينترنت با يک آدرس IP

آدرس IP

- 32 بيتي
- پرارزشترين بايت آدرس IP مشخص كننده كلاس آدرس
- نوشتن آدرسهاي IP به صورت چهار عدد دهدهي كه با نقطه از هم جدا شده اند جهت سادگي نمايش

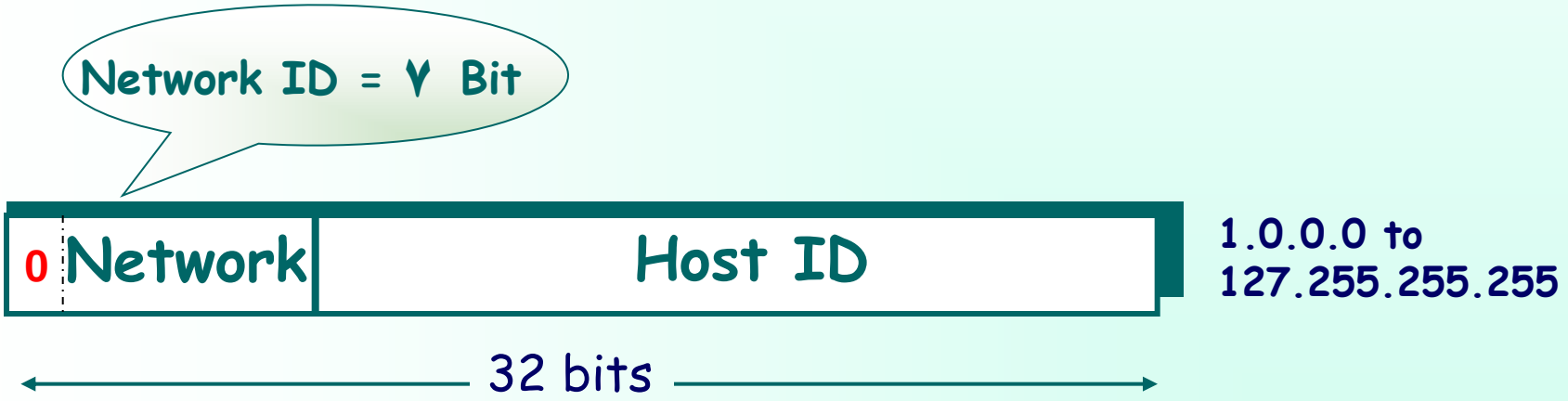


تقسیم ۳۲ بیت آدرس IP به قسمتهای :

آدرس ماشین/ آدرس زیرشبکه/ آدرس شبکه

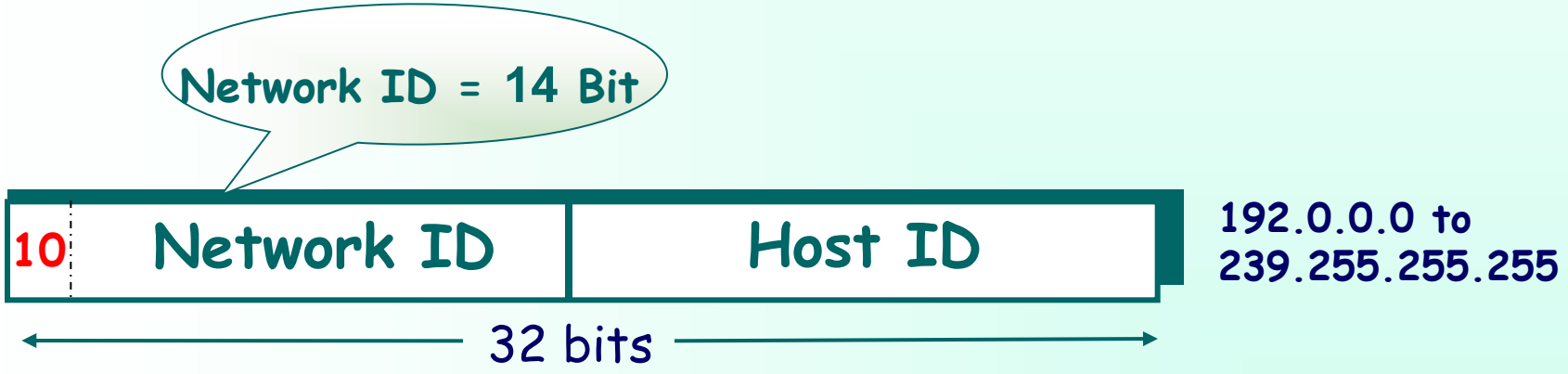
آدرسهای کلاس A

- مقدرا پرارزشترین بیت = 0
- 7 بیت از یک بایت اول = مشخصه آدرس IP
- 3 بایت باقیمانده مشخص‌کننده آدرس ماشین میزبان
- بایت پرارزش در محدوده صفر تا 127



کلاس B

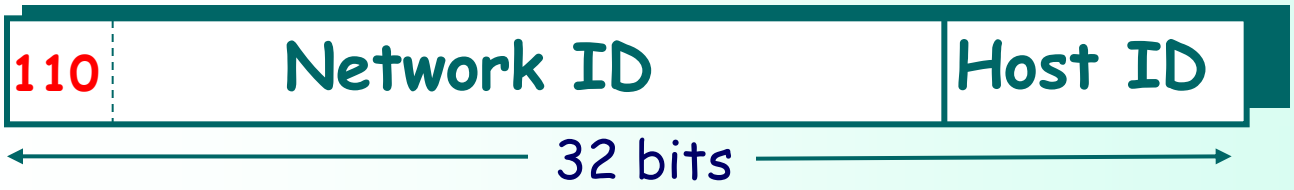
- مقدار دو بیت پرارزش = 10
- 14 بیت از دو بایت سمت چپ = آدرس شبکه
- دو بایت اول از سمت راست = آدرس ماشین میزبان



192.0.0.0 to
239.255.255.255

کلاس C

- مناسب‌ترین و پرکاربردترین کلاس از آدرسهاي IP
- مقدار سه بیت پرارزش = 110
- 21 بیت از سه بایت سمت چپ = مشخص‌کننده آدرس شبکه
- 8 بیت سمت چپ = آدرس ماشین میزبان



240.0.0.0 to
247.255.255.255

کلاس D

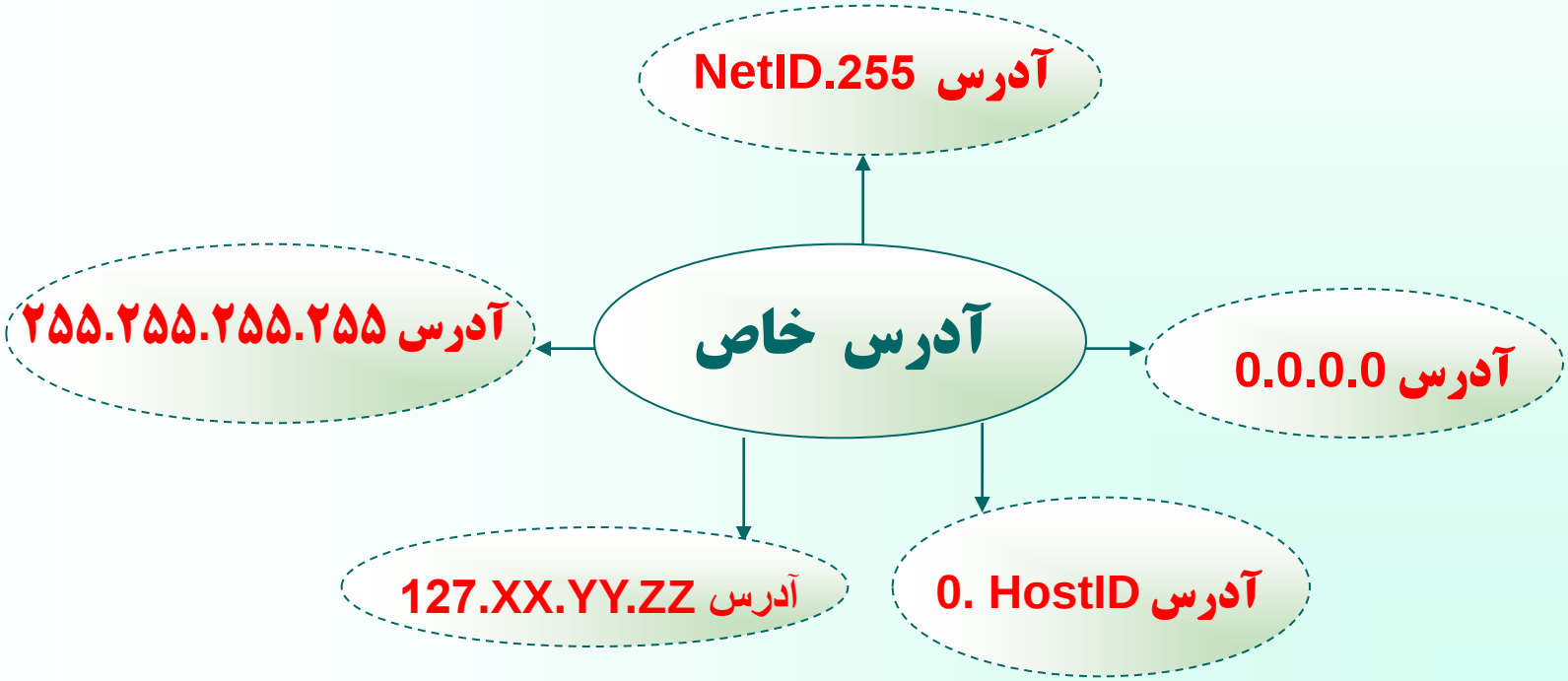
- مقدار چهار بيت پرارزش = 1110
- 28 بيت = تعيين آدرسهاي چند مقصده (آدرسهاي گروهي)
- كاربرد = عمليات رسانه‌اي و چند پخشي

کلاس E

- مقدار پنج بیت پرارزش = 11110

آدرسهای خاص

در بین تمام کلاسهاي آدرس IP با پنج گروه از آدرسها نمي توان يک شبکه خاص را تعريف و آدرس‌دهي نمود.



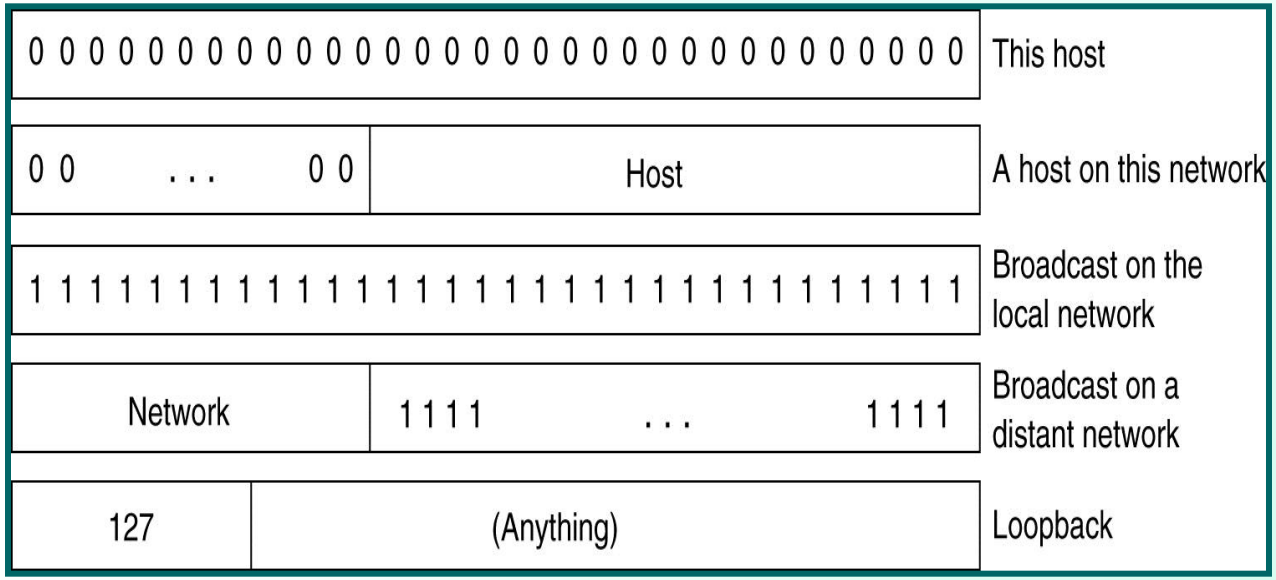
آدرس 0.0.0.0:

هر ماشين ميزبان كه از آدرس IP خودش مطلع نيست اين آدرس را بعنوان آدرس خودش فرض مي‌كند.

آدرس HostID 0. :

اين آدرس زماني به كار مي‌رود كه ماشين ميزبان ، آدرس مشخصة شبكه‌اي كه بدان متعلق است را نداند. در اين حالت در قسمت NetID مقدار صفر و در قسمت HostID شمارة مشخصة ماشين خود را قرار مي‌دهد.

0



آدرس 255.255.255.255:

جهت ارسال پيامهاي فراگير براي تمامي ماشينهاي ميزبان بر روي شبكة محلي كه ماشين ارسال‌كننده به آن متعلق است .

آدرس NetID.255 :

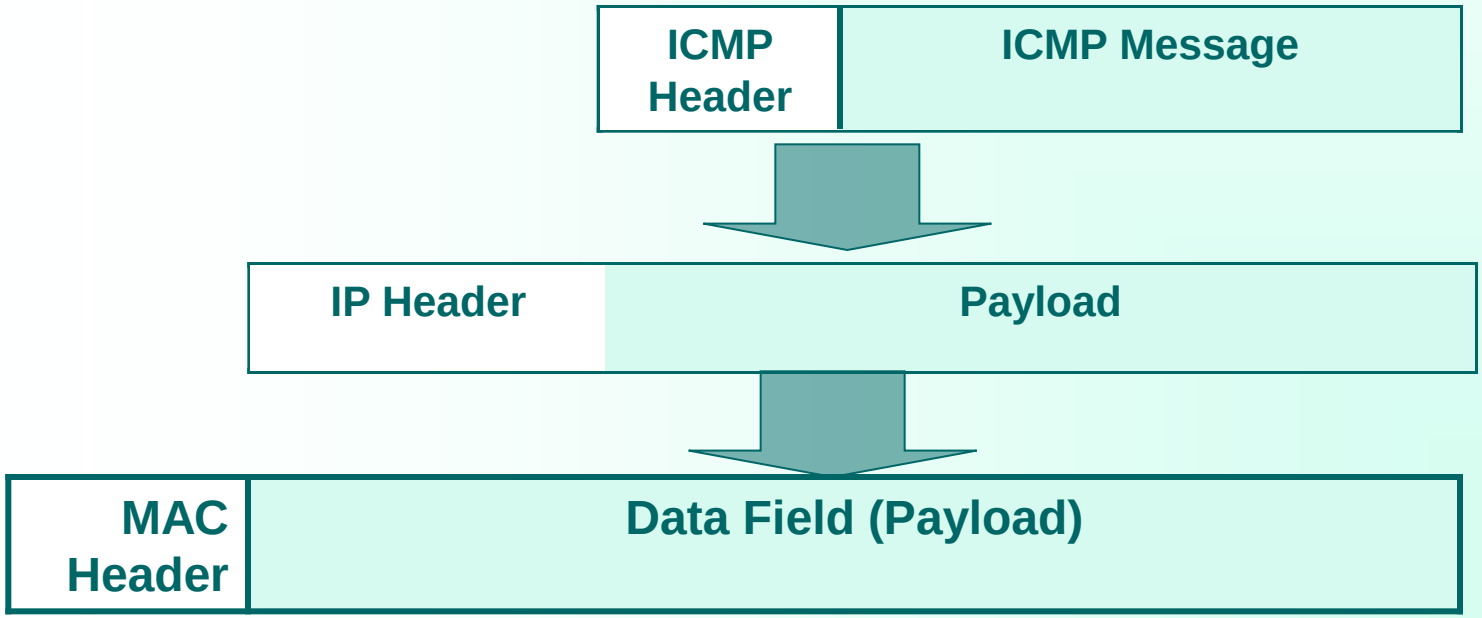
جهت ارسال پيامهاي فراگير براي تمامي ماشينهاي يك شبكة راه دور كه ماشين ميزبان فعلي متعلق به آن نيست .

آدرس 127.xx.yy.zz:

اين آدرس بعنوان "آدرس بازگشت" شناخته مي‌شود و آدرس بسيار مفيدي براي اشكالزدايي از نرم افزار مي‌باشد .

پروتکل ICMP: Internet Control Message Protocol

- بررسي انواع خطا و ارسال پيام براي مبدأ بسته در صورت بروز خطا و اعلام نوع خطا
- يك سيستم گزارش خطا
- قرارگرفتن پيام ICMP درون بسته IP

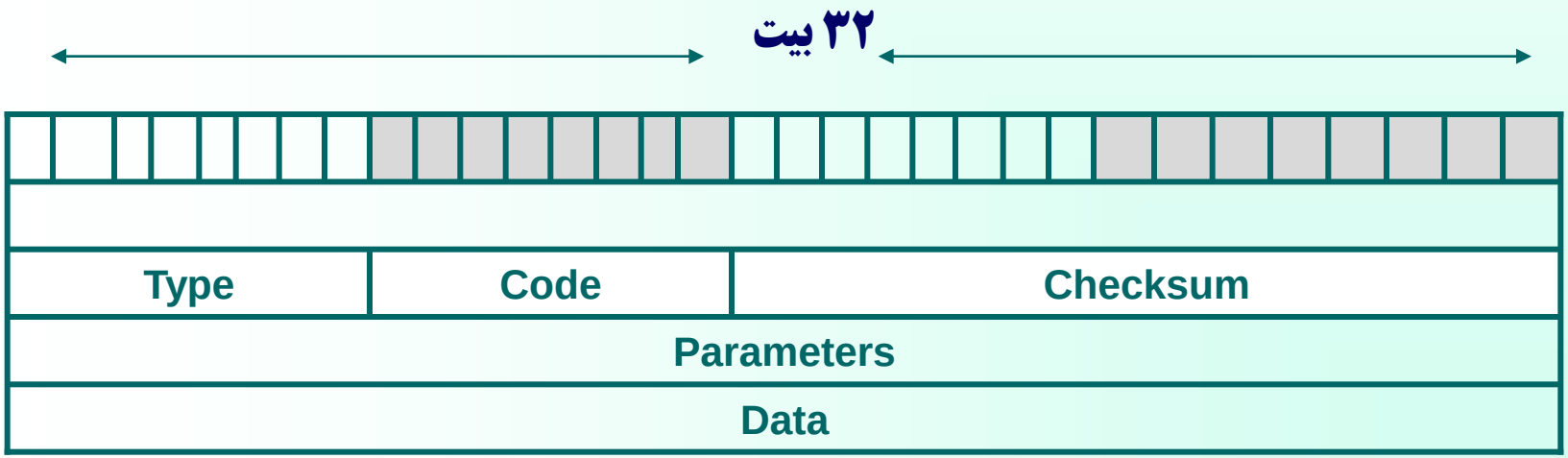


قالب پیام ICMP

فیلد **Type**: مشخص کننده نوع پیام

فیلد **Code**: مشخص کننده کد زیرنوع

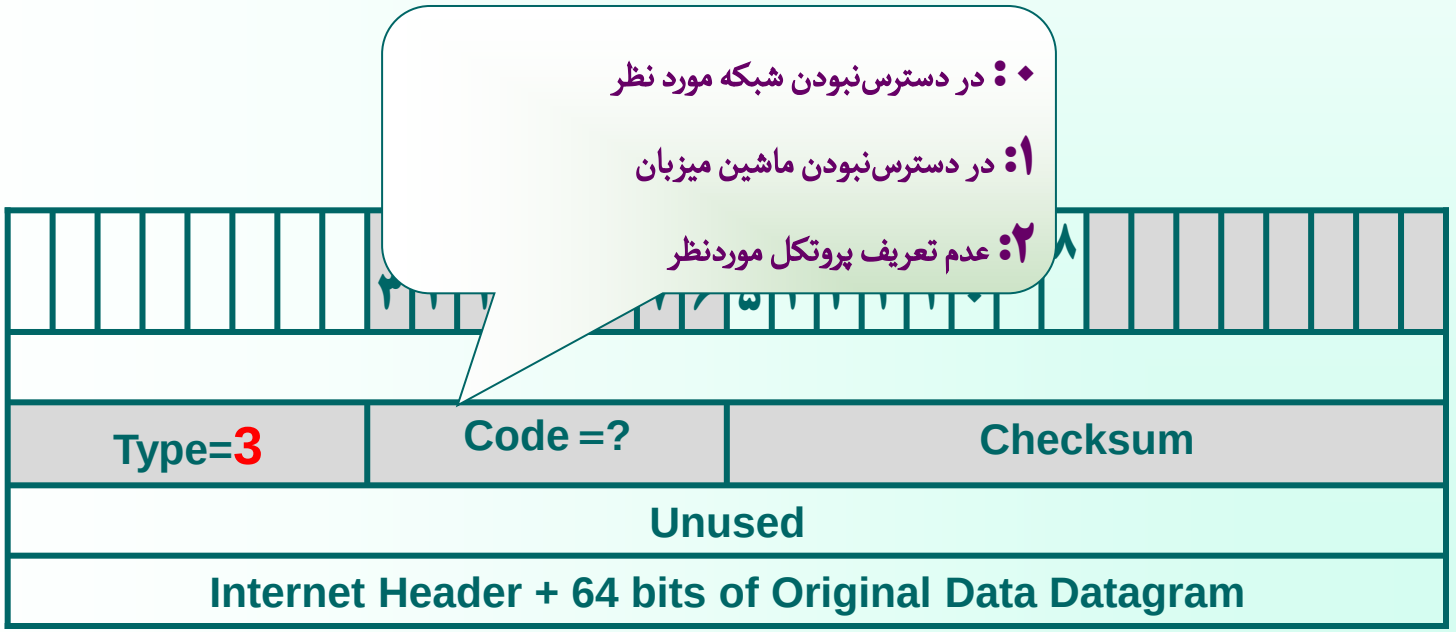
فیلد **Checksum**: جهت سنجش اعتبار و درستي بسته ICMP



انواع پیامهای ICMP

1) پیام Destination Unreachable

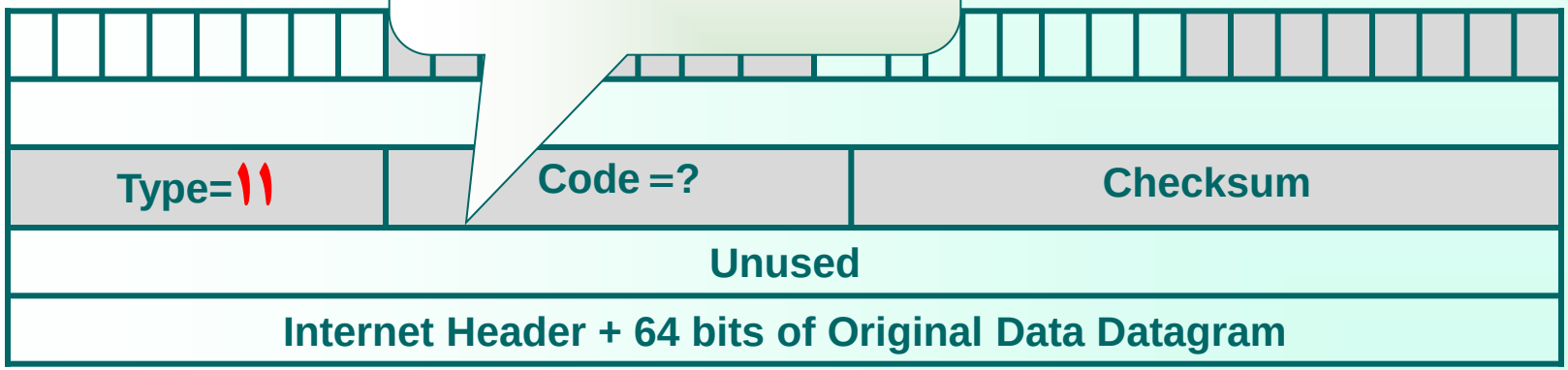
- عدم تشخیص آدرس توسط مسیریاب و یا زیر شبکه
- نرسیدن بسته به مقصد به هر علت



۲) پیام Time Exceeded

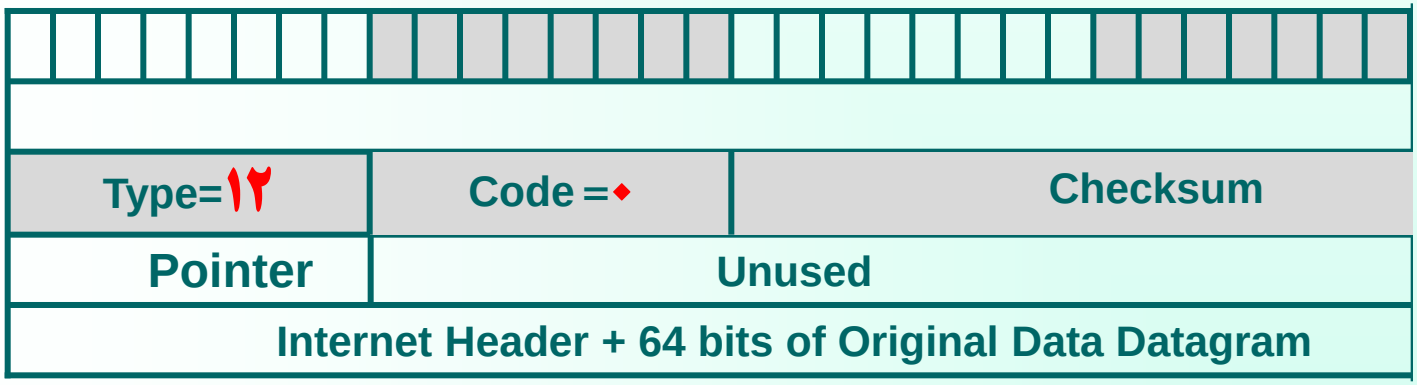
ارسال پیام به فرستنده بسته جهت آگاهي از اتمام طول عمر بسته و حذف آن توسط مسیریاب

- ۰ = اتمام زمان حیات بسته
- ۱= اتمام زمان بازسازي قطعات يك ديتاگرام



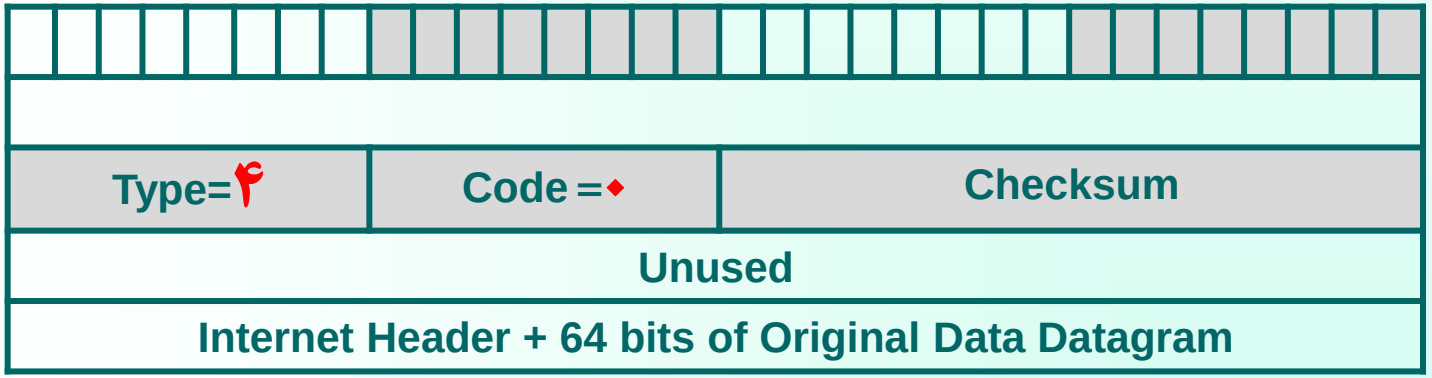
۳) پیام Parameter Problem

نشان‌دهنده وجود مقدار نامعتبر در یکي از فیلدهاي سرآیند بسته IP



۴) پیام Source Quench

تقاضاي كاهش نرخ توليد و ارسال بسته‌هاي IP از ماشين ميزبان



۵) پیام Redirect

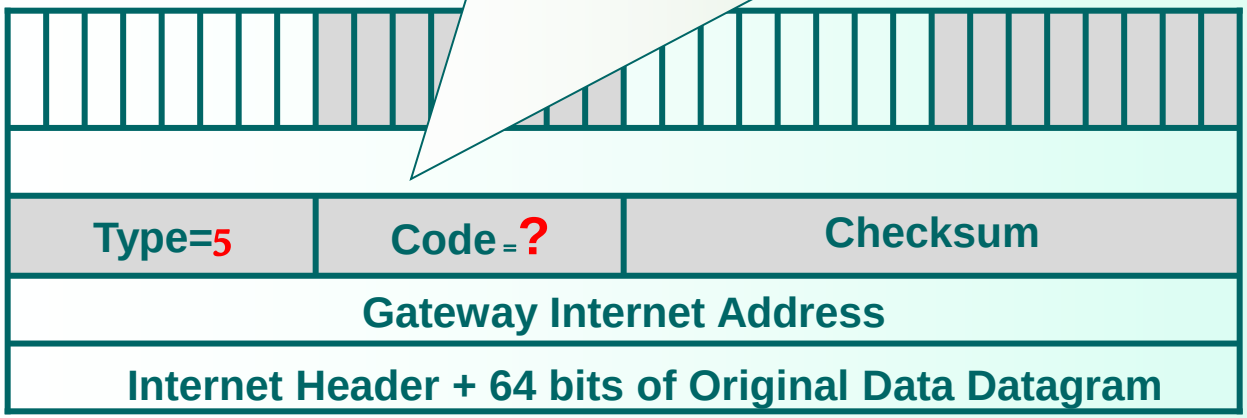
وجود اشکال در مسیریابي

0 = تغییر مسیر به شبکه‌اي که آدرس آن مشخص شده است.

1 = تغییر مسیر به ماشیني که آدرس آن مشخص شده است.

2 = تغییر مسیر به شبکه‌اي که آدرس آن مشخص شده است جهت تأمین سرویس ویژة درخواستي مشخص شده در فیلد **Type of service**

3 = تغییر مسیر به ماشیني که آدرس آن مشخص شده است جهت تأمین سرویس ویژة درخواستي مشخص شده در فیلد **Type of service**



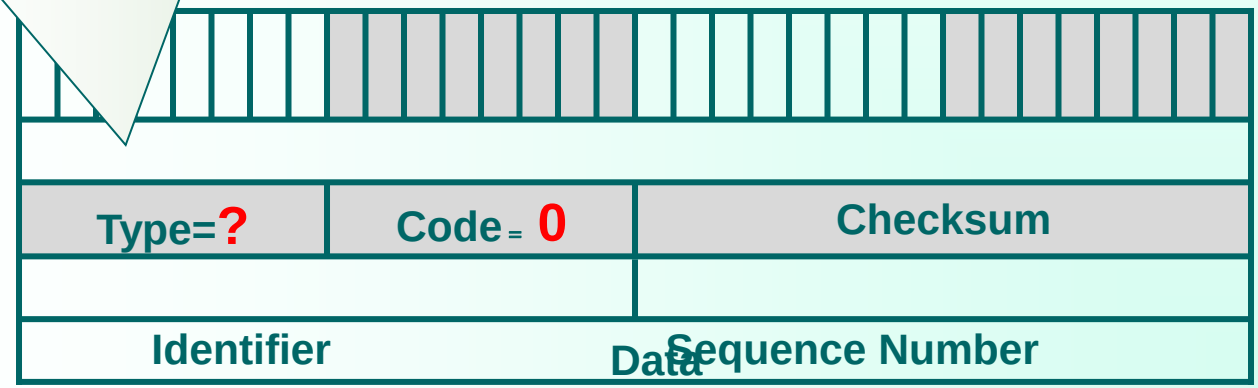
6) پيامهاي Echo Request , Echo Reply

پيام Echo Request : موجود و قابل دسترس بودن يك ماشين خاص در شبكه توسط مسيرياب

پيام Echo Reply: پاسخ مقصد مبني بر دريافت پيام Echo Request

Echo Request : براي مشخص كردن پيام 8

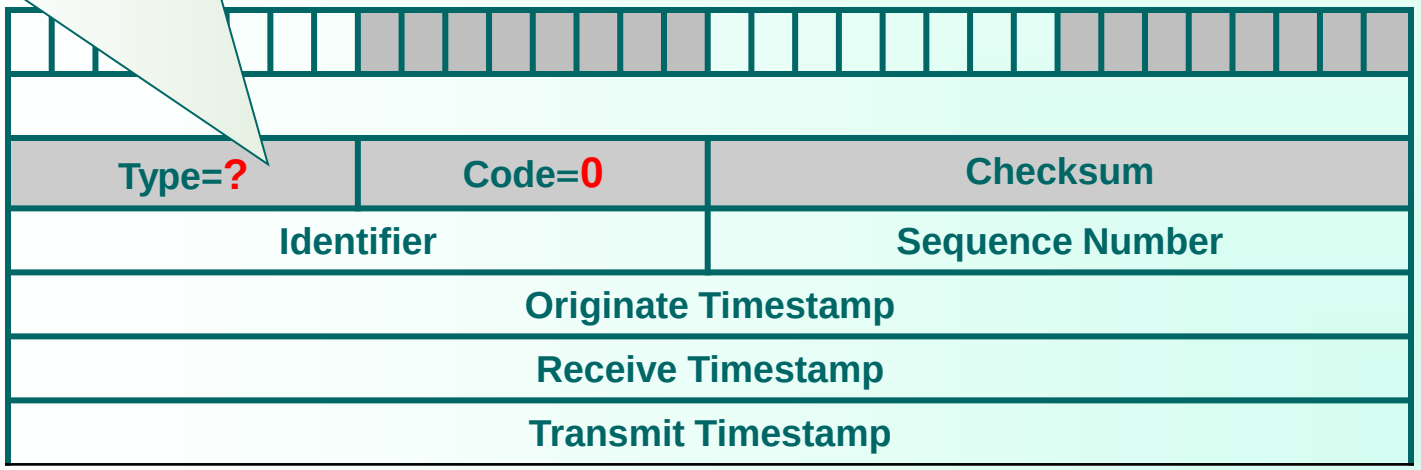
Echo Reply : براي مشخص كردن پيام 0



7) پيامهاي Timestamp Reply و Timestamp Request

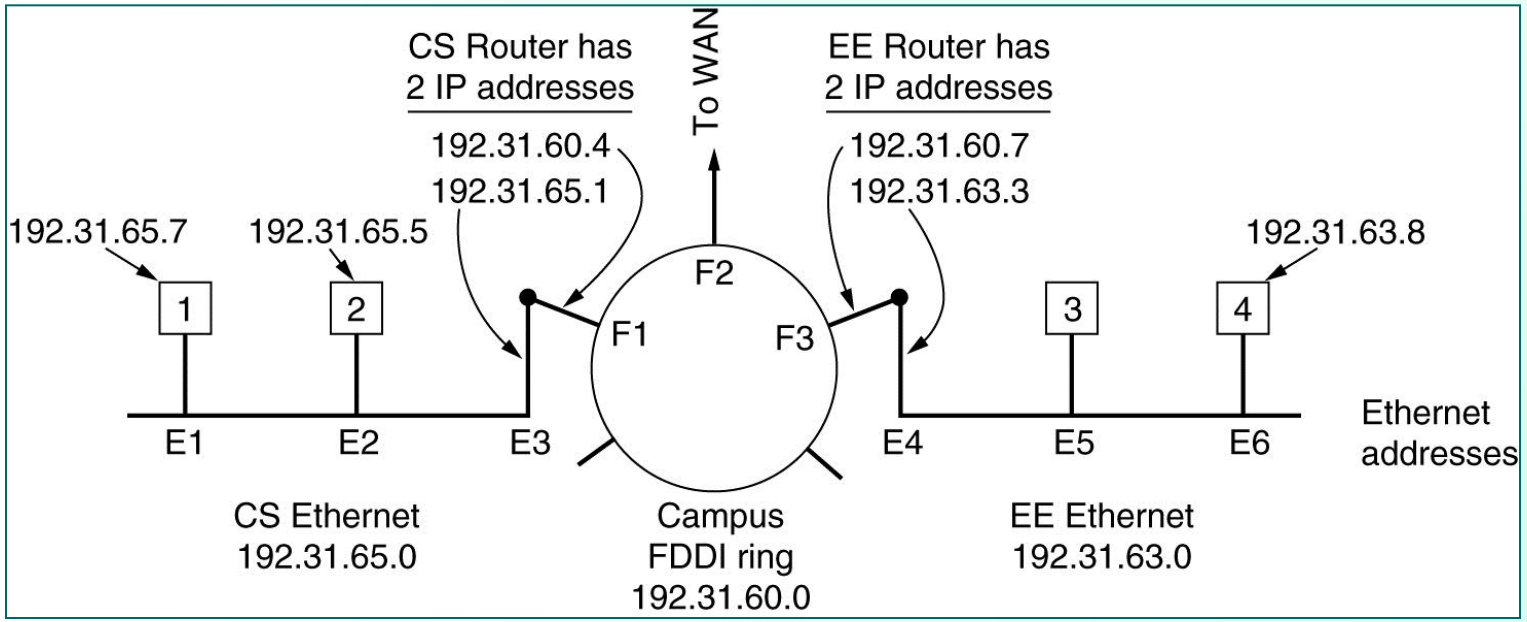
دريافت‌كننده پيام Timestamp Request زمان دريافت و زمان ارسال بسته را نيز مشخص مي‌كند.

13 : براي مشخص كردن پيام Timestamp Request
14 : براي مشخص كردن پيام Timestamp Reply

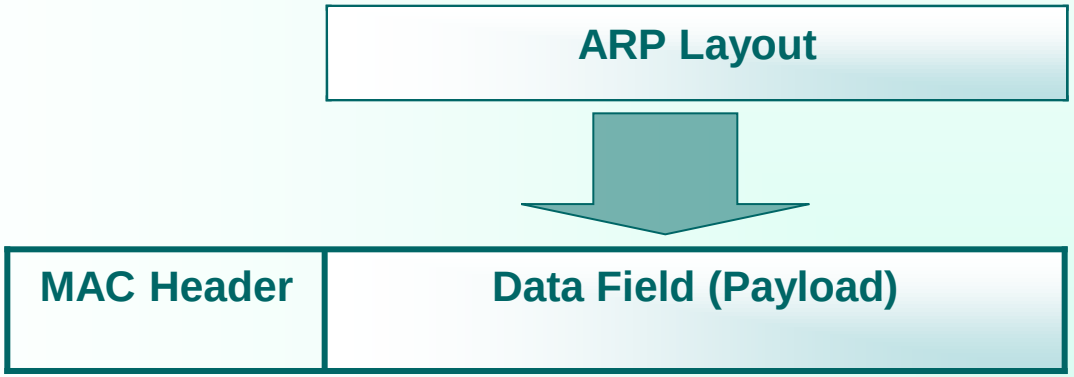


پروتکل ARP : Address Resolution Protocol

- بي‌معنابودن آدرسهاي IP روي كانال انتقال
- دانستن آدرس IP ماشين مقصد و نياز به داشتن آدرس فيزيكي آن جهت ارسال بسته
- وظيفه پروتكل ARP:
- ارسال بسته فراگير روي كل شبكه محلي كه در آن آدرس IP ماشين مورد نظر قرار دارد. پاسخ ماشين با آدرس IP موجود در بسته ارسالي و ارسال آدرس فيزيكي خود براي ارسال‌كننده بسته ARP

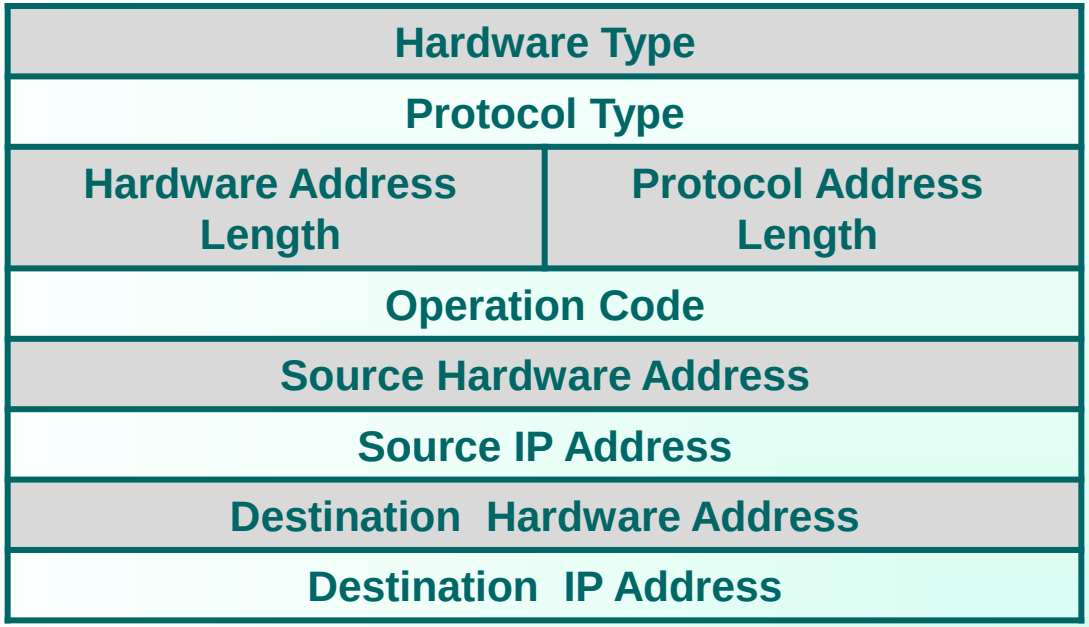


برخلاف پروتكل ICMP كه روي پروتكل IP قرار مي‌گيرد ، پروتكل ARP مستقيماً بر روي پروتكل لاية فيزيكي عمل مي‌كند ؛ يعني يك بستة ARP ساخته شده و درون فيلد داده از فريم لاية فيزيكي قرار گرفته و روي كانال ارسال مي‌شود .



چگونگي قرار گرفتن يك پيام ARP درون فريم لاية فيزيكي

ساختار پیامهای ARP



پروتكل *RARP* : Reverse Address Resolution Protocol

- ايستگاه آدرس فيزيكي مورد نظرش را مي‌داند وليكن آدرس IP آن را نمي‌داند
- ارسال يك بسته فراگير روي خط
- تمامي‌ايستگاههايي كه از پروتكل RARP حمايت مي‌كنند و بسته‌هاي مربوطه را تشخيص مي‌دهند ، در صورتي كه آدرس فيزيكي خودشان را درون بسته ببينند در پاسخ به آن ، آدرس IP خود را در قالب يك بستة RARP Reply برمي‌گردانند.

توجه: بسته‌هاي RARP, ARP از نوع فراگير محلي Local Broadcast هستند و بالطبع توسط مسيريابها منتقل نمي‌شوند و فقط در محدوده شبكه محلي عمل مي‌كنند.

.

پروتكل *BootP*

- گاهي نياز است كه يك آدرس IP روي چند شبكه محلي جستجو شود كه در اين حالت RARP جوابگو نيست .
- داشتن آدرس فيزيكي ماشين مورد نظر و نياز به پيداكردن آدرس IP ان در شبكه‌هاي محلي ديگر
- استفاده از بسته‌هاي UDP در اين پروتكل

فصل دوم : مسیریابی در شبکه اینترنت

هدفهای آموزشی :

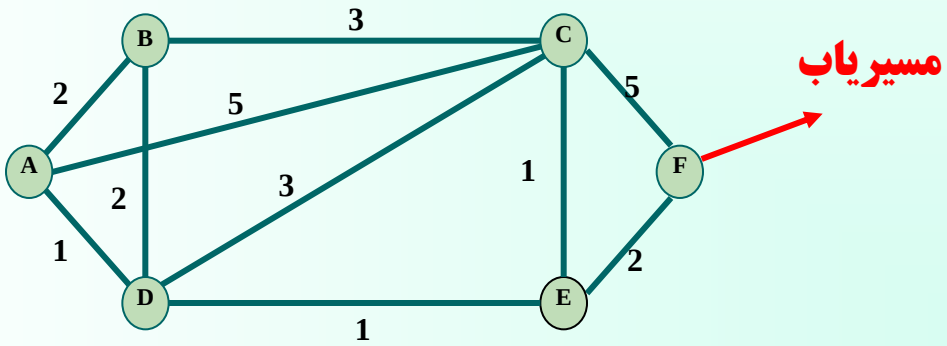
- مفاهیم اولیه مسیریابی
- الگوریتم‌های مسیریابی LS
- الگوریتم‌های مسیریابی بردار فاصله - DV -
- مسیریابی سلسله مراتبی
- پروتکل RIP
- پروتکل OSPF
- پروتکل BGP

۱) مفاهیم اولیه مسیریابی

مسیریاب: ابزاري است براي برقراري ارتباط دو يا چند شبكه

زيرساخت ارتباطي: مجموعه مسيريابها و كانالهاي فيزيكي ما بين آنها

الگوريتم‌هاي مسيريابي : روشهايي براي پيدا كردن مسيري بهينه ميان دومسيرياب به گونه‌اي كه هزينه كل مسير به حداقل برسد.



زیرساخت ارتباطی یک شبکهٔ فرضی

برخی اصطلاحات کلیدی در مسیریابی

آدرسهاي MAC:

- آدرسهاي لايه فيزيكي جهت انتقال فريمها بر روي كانال
- اندازه آدرس وابسته به پروتكل و توپولوژي شبكه
- تغيير آدرسهاي MAC بسته‌هاي اطلاعاتي هنگام عبور از مسيريابهاي موجود در مسير

آدرسهاي IP :

- آدرسهاي جهاني و منحصر به فرد
- مشخص‌كننده يک ماشين فارغ از نوع سخت افزار و نرم افزار آن
- ثابت بودن آدرسهاي IP بسته هاي اطلاعاتي هنگام عبور از مسيريابهاي موجود در مسير

بسته IP:

- واحد اطلاعاتي با اندازه محدود

توپولوژي شبكه:

- مجموعه مسيريابها و كانالهاي فيزيكي ما بين آنها در زيرساخت ارتباطي يك شبكه
- متغير با زمان

ترافيك شبكه:

- تعداد متوسط بسته‌هاي اطلاعاتي ارسالي و يا دريافتي روي يك كانال در واحد زمان
- متغير با زمان

گام يا Hop:

- عبور بسته از يك مسيرياب = گام
- تعداد مسيريابهاي موجود در مسير يك بسته = تعداد گام = **Hop Count**

ازدحام يا Congestion:

بيشتر بودن تعداد متوسط بسته‌هاي ورودي به يك مسيرياب از تعداد متوسط بسته هاي خروجي

بن بست Deadlock:

پايان طول عمر بسته‌ها

۱–۱) روشهای هدایت بسته‌های اطلاعاتی در شبکه‌های کامپیوتری

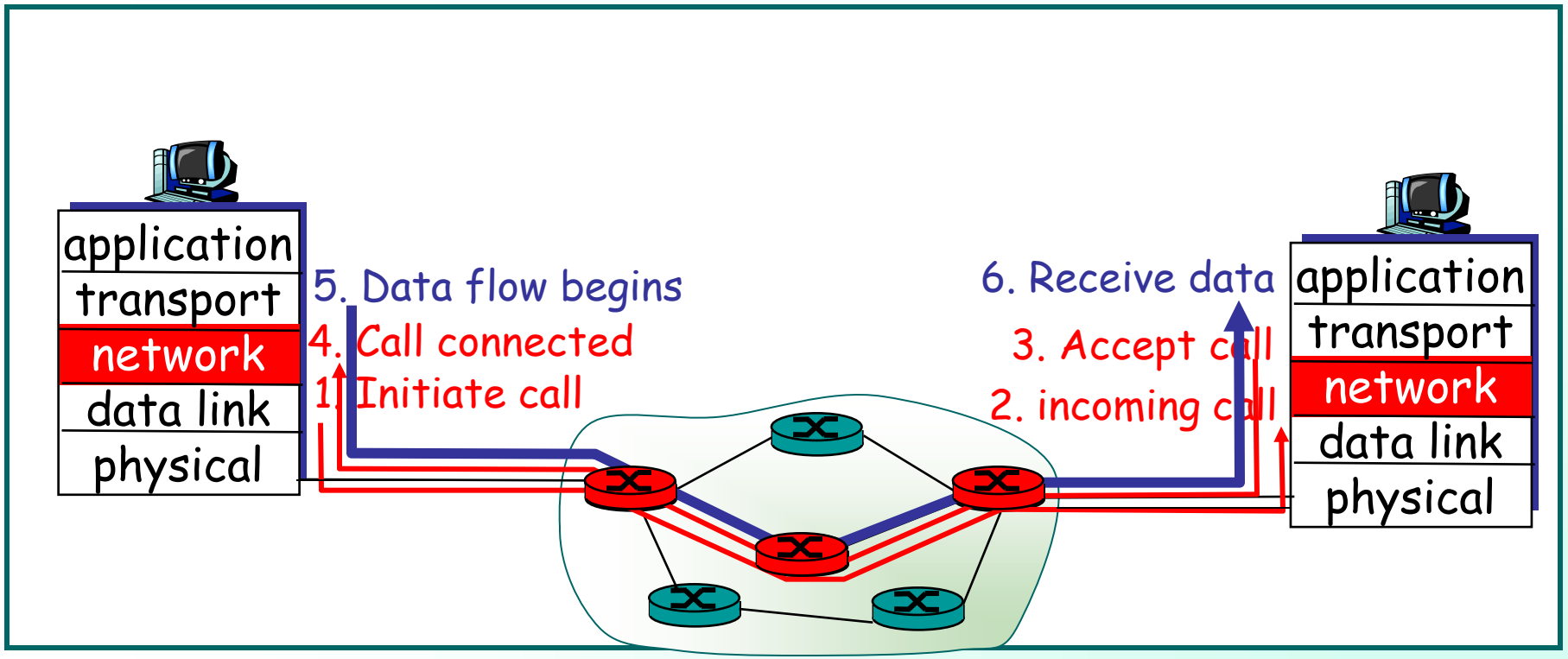
الف) روش مدار مجازي Virtual Circuit (VC)

ب) روش ديتاگرام Datagram

خصوصیات روش VC

- ارسال بسته‌هاي اطلاعاتي بدون نياز به اطلاع از آدرسهاي IP مبدأ و مقصد و فقط داشتن شماره VC جهت ارسال بسته
- عدم اجراي الگوريتم مسيريابي جهت هدايت بسته‌هاي اطلاعاتي از مبدأ به مقصد
- دريافت بسته به ترتيب ارسال شده در مقصد
- عدم احتمال گم‌شدن بسته‌ها در عمل مسيريابي در شبكه

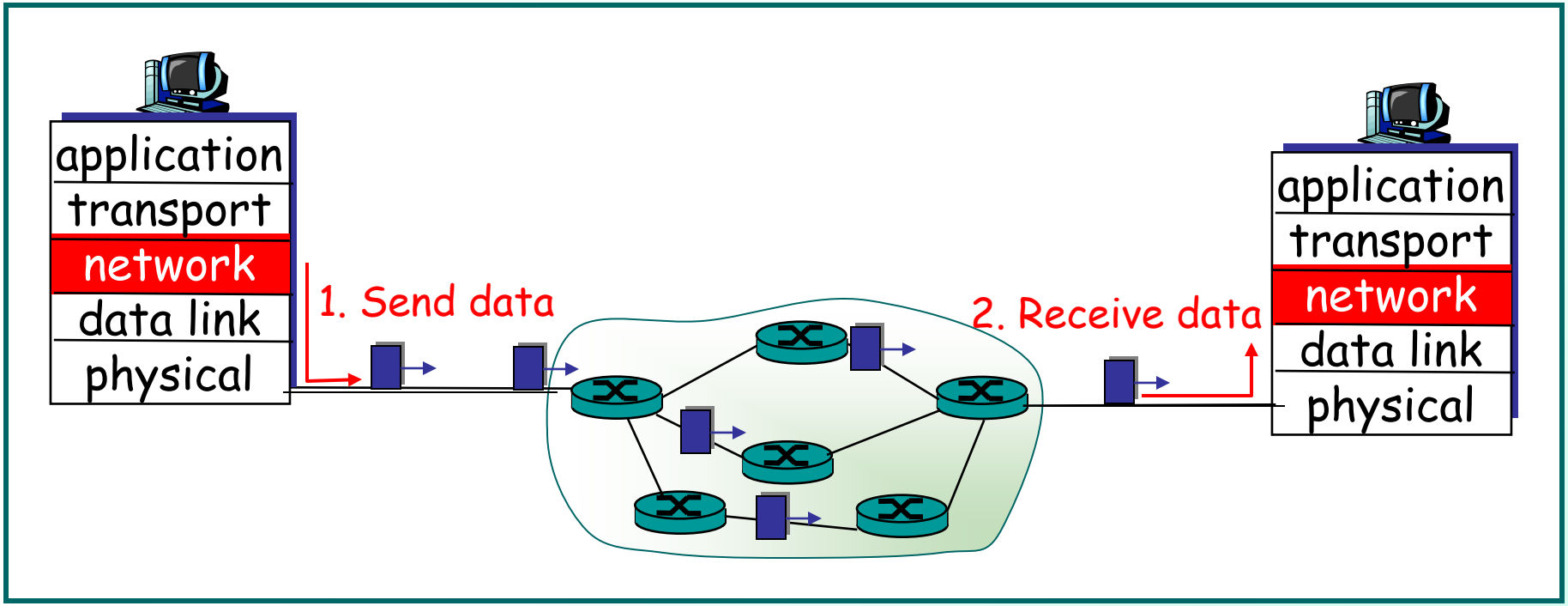
روش vc


application
transport
network
data link
physical
5. Data flow begins
4. Call connected
1. Initiate call
6. Receive data
3. Accept call
2. incoming call
application
transport
network
data link
physical

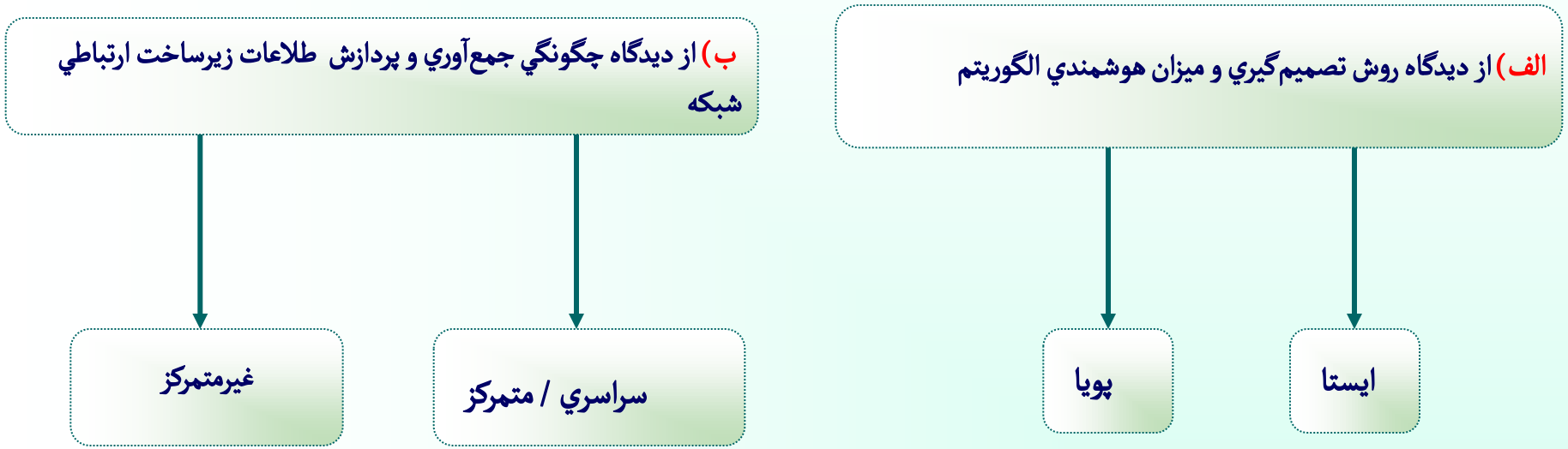
خصوصيات روش ديتاگرام

- ارسال بسته‌هاي اطلاعاتي با استفاده از آدرسهاي IP مبدأ و مقصد در شبكه
- انجام مسيريابي جداگانه براي هر بسته
- توزيع و هدايت بسته‌ها روي مسيرهاي متفاوت بر اساس شرايط توپولوژيكي و ترافيكي لحظه‌اي شبكه
- امكان دريافت بسته بدون ترتيب ارسال شده در مقصد
- لزوم نظارتهاي ويژه بر گم شدن و يا تكراري بودن بسته در لايه‌هاي بالاتر

روش Datagram



انواع الگوریتمهای مسیریابی



الگوريتم ايستا

- عدم توجه به شرايط توپولوژيكي و ترافيك لحظه‌اي شبكه
- جداول ثابت مسيريابي هر مسيرياب در طول زمان
- الگوريتم‌هاي سريع
- تنظيم جداول مسيريابي به طور دستي در صورت تغيير توپولوژي زيرساخت شبكه
- تغيير مسيرها به كندي در اثناي زمان

الگوريتم پويا

- به هنگام سازي جداول مسيريابي به صورت دوره‌اي بر اساس آخرين وضعيت توپولوژيكي و ترافيك شبكه
- تغيير سريع مسيرها
- تصميم‌گيري بر اساس وضعيت فعلي شبكه جهت انتخاب بهترين مسير
- ✕ ايجاد تأخيرهاي بحراني هنگام تصميم‌گيري بهترين مسير به جهت پيچيدگي الگوريتم

الگوريتم سراسری

- اطلاع كامل تمام مسيريابها از همبندي شبكه و هزينه هر خط
- الگوريتم‌هاي Link State (LS)

الگوريتم غير متمركز

- محاسبه و ارزيابي هزينه ارتباط با مسيريابهاي همسايه (مسيريابهايي كه به صورت مستقيم و فيزيكي با آن در ارتباط هستند)
- ارسال جداول مسيريابي توسط هر مسيرياب در فواصل زماني منظم براي مسيريابهاي مجاور
- پيچيدگي زماني كم
- الگوريتم‌هاي Distance Vector

۳–۱) روش ارسال سیل آسا (Flooding Algorithm)

- سريعترين الگوريتم براي ارسال اطلاعات به مقصد در شبكه
- جهت ارسال بسته‌هاي فراگير و كنترلي مانند اعلام جداول مسيريابي

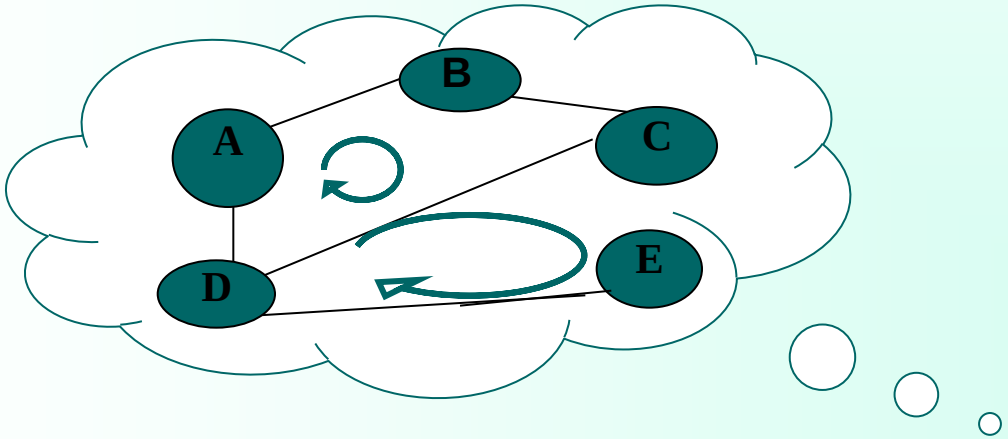
مشکل روش سیل آسا

- ایجاد حلقه بینهایت و از کارافتادن شبکه

راه حل رفع مشکل حلقه بینهایت

1) قراردادن شماره شناسايي براي هر بسته Selective Flooding

2) قراردادن طول عمر براي بسته‌ها



حلقه‌هاي بينهايت در روش سيل آسا

الگوريتم هاى LS

1- شناسايي مسيريابهاي مجاور

2- اندازه‌گيري هزينه

3- تشكيل بسته‌هاي LS

4- توزيع بسته‌هاي LS روي شبكه

5- محاسبه مسيرهاي جديد

1- شناسايي مسيريابهاي مجاور

- ارسال بسته خاصي به نام بسته سلام Hello Packet توسط مسيرياب به تمام خروجي‌ها
- پاسخگويي مسيريابهاي متصل از طريق كانال فيزيكي مستقيم به بسته ارسالي و اعلام آدرس IP خود به مسيرياب
- درج اطلاعات بسته‌هاي پاسخ در جدول مسيرياب

2- اندازه‌گيري هزينه

- اندازه‌گيري تأخير هر يك از خطوط خروجي مسيرياب توسط خود مسيرياب
- ارسال بسته خاص به نام Echo Packet روي تمام خطوط خروجي خود
- پاسخ تمام مسيريابهاي گيرنده بسته با ارسال بسته Echo Reply
- اگر مسيرياب موظف باشد كه با دريافت بستة Echo خارج از نوبت و به سرعت به آن پاسخ بدهد ، "زمان رفت و برگشت" اين بسته فقط تاخير فيزيكي بين دو مسيرياب را به عنوان معيار هزينه مشخص مي‌كند.
- اندازه‌گيري اين زمان با استفاده از زمان سنج و تقسيم آن مقدار بر عدد 2 و درج در جدول توسط مسيرياب

3- تشكيل بسته‌هاي LS

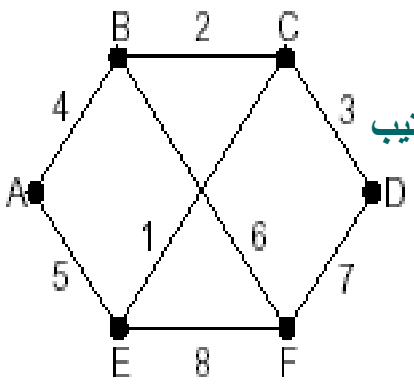
تشكيل بسته LS پس از جمع آوري اطلاعات لازم از مسيريابهاي مجاور شامل:

الف) آدرس جهاني مسيرياب توليدكنندة بسته

ب) يك شمارة ترتيب (تا بسته‌هاي تكراري از بسته‌هاي جديد تشخيص داده شوند.)

ج) طول عمر بسته (تا اطلاعات بسته ، زمان انقضاي اعتبار داشته باشد.)

د) آدرس جهاني مسيريابهاي مجاور و هزينة تخميني



فيلد شماره ترتيب

فيلد طول عمر

A	
Seq.	
Age	
B	4
E	5

Link	
B	
Seq.	
Age	
A	4
C	2
F	6

State	
C	
Seq.	
Age	
B	2
D	3
E	1

D	
Seq.	
Age	
C	3
F	7

Packets	
E	
Seq.	
Age	
A	5
C	1
F	8

F	
Seq.	
Age	
B	6
D	7
E	8

يك زيرساخت از يك شبكه فرضي

بسته‌هاي LS

4- توزيع بسته‌هاي LS روي شبكه

- ارسال بسته‌هاي LS به روش سيل آسا
- وجود شماره ترتيب براي هر بسته جهت جلوگيري از بروز حلقه تكرار
- در نظرگرفتن طول عمر براي هر بسته جهت رفع مشكل دريافت بسته‌هاي تكراري
- احراز هويت ارسال‌كننده بسته LS در مسيريابها جهت جلوگيري از بسته‌هاي LS آلوده

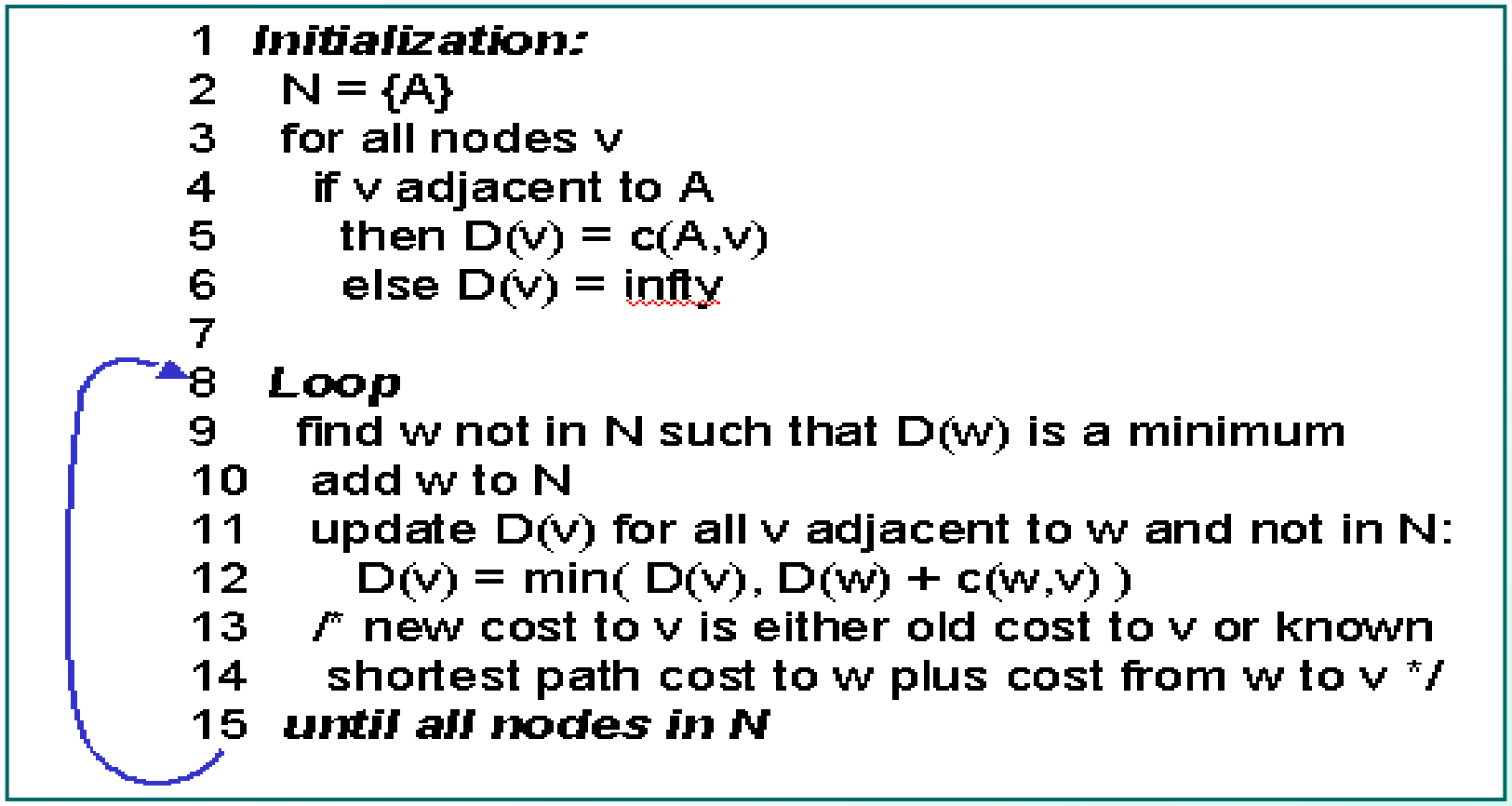
5- محاسبه مسيرهاي جديد

- تشكيل ساختمان داده گراف زيرشبكه جهت انتخاب بهترين مسير بين دو گره هنگام دريافت بسته‌هاي LS از تمام مسيريابهاي شبكه
- استفاده از الگوريتم دايجكسترا جهت يافتن بهترين مسير بين دو گره

(Dijkstra Shortest Path Algorithm)

* C(i , j) بيانگر هزينه خط ميان گره i تا j است.
  هرگاه همسايگاني در مجاورت گره وجود نداشته باشند
  C(i , j) بينهايت تلقي مي شود.
* D(v) هزينه فعلي مسير ميان مبدا تا گره V.
* P(v) گره‌اي كه در طول مسير از مبدا تا V درست قبل از V واقع شده.
* N مجموعه گره‌هايي كه عبور از آنها كم هزينه برآورد گشته است.

Dijkstra's Algorithm



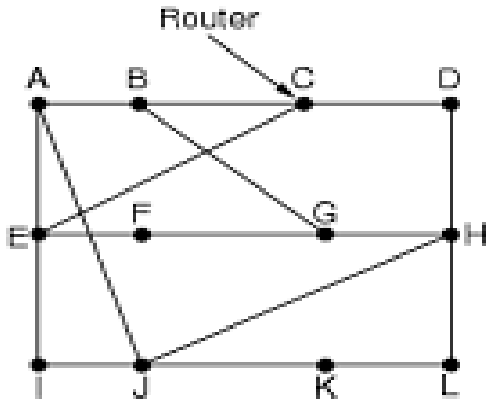
الگوریتمهای DV یا بردار فاصله

- يكي از روشاي پويا در مسيريابي
- مورد استفاده در شبكه ARPA
- استفاده در مسيريابهاي كوچك
- نامهاي متفاوت روش DV
- پروتكل RIP
- الگوريتم مسيريابي Bellman - Ford
- الگوريتم مسيريابي Ford – Fulkerson
- الگوريتم Distance Vector Routing

اصول کار روش DV

- محاسبه خطوطي را كه به صورت فيزيكي با مسيريابهاي ديگر دارد و درج در جدول مسيريابي
- بينهايت درنظرگرفتن هزينة خطوطي كه مسيرياب با آنها در ارتباط مستقيم نيست
- ارسال ستون هزينه از جدول مسيريابي براي مسيريابهاي مجاور در بازه‌هاي زماني مشخص ، توسط هر مسيرياب (“يعني فقط براي مسيريابهائي كه با آن در ارتباط است نه تمام مسيريابها ”). دريافت اطلاعات جديد ا زمسيريابهاي مجاور در در فواصل T ثانيه‌اي
- به هنگام نمودن جدول مسيريابي پس از دريافت جداول مسيريابي از مسيريابهاي مجاور ، طبق يك الگوريتم بسيار ساده

الگوریتمهای DV یا بردار فاصله



(a)

زیرساخت ارتباطی یک شبکهٔ فرضی
با دوازده مسیریاب

To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	—
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J	

Vectors received from J's four neighbors

(b)

جدول مسیریابی مربوط به مسیریاب J

مشکل عمده پروتکلهای DV

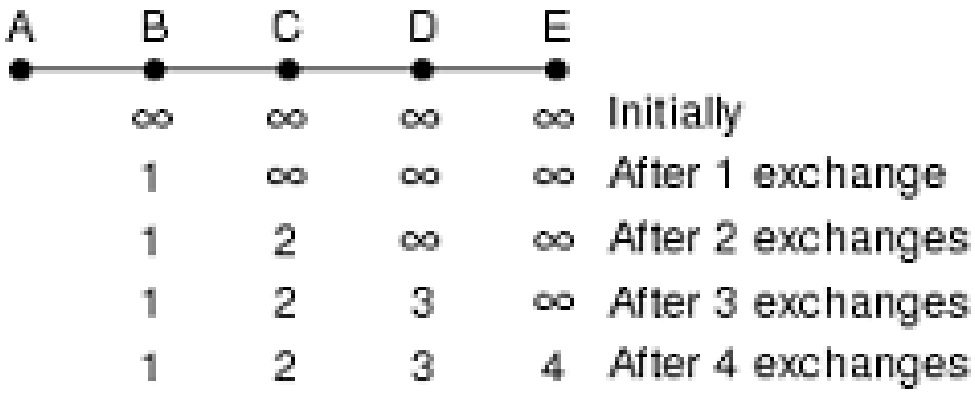
عدم همگرايي سريع جداول مسيريابي هنگام خرابي يك مسيرياب يا يك كانال ارتباطي = مشكل شمارش تا بينهايت

راه حل :

وقتي يك مسيرياب مي‌خواهد اطلاعاتي را به همسايه‌هايش بدهد هزينه رسيدن به آنهايي را كه قطعاً بايد از همان مسيرياب بگذرند را اعلام نمي‌كند. (يا ∞ اعلام مي‌كنند)

مسئله شمارش تا بينهايت

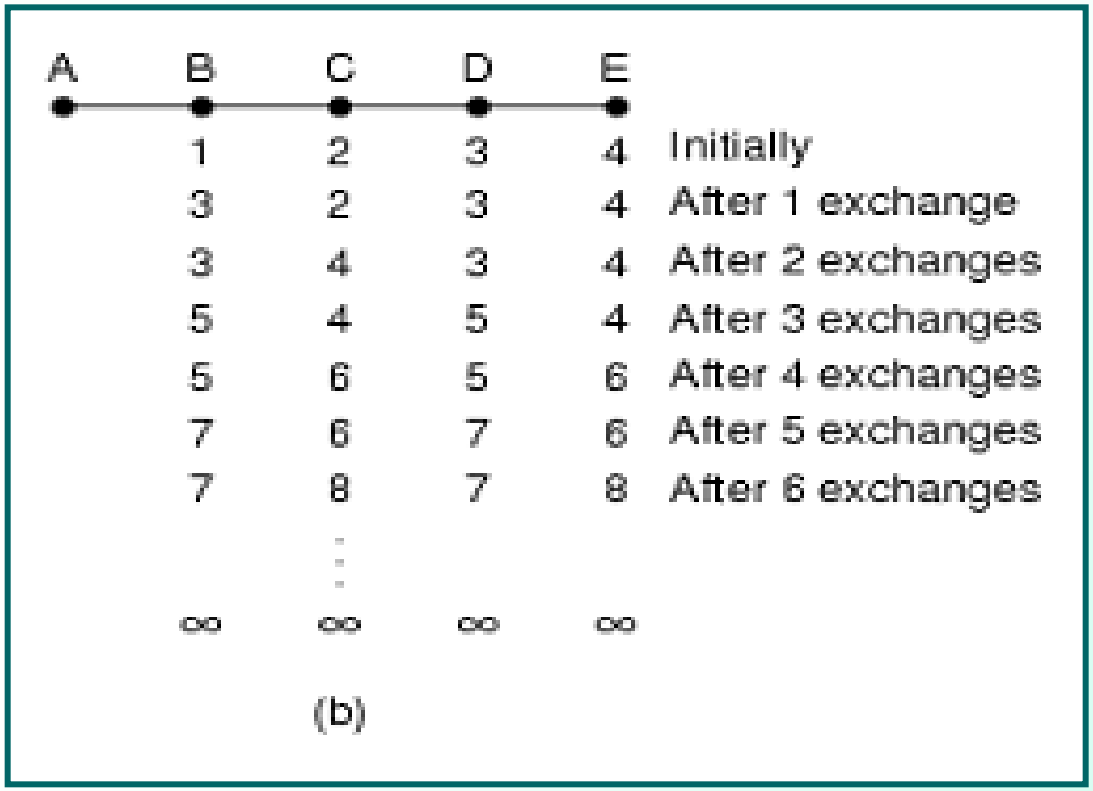
به خبرهاي خوب واكنش سريع ولي به خبرهاي بد واكنش كندي نشان مي دهد.



The count-to-infinity problem.

مسئله شمارش تا بینهایت

هرگاه مسيريابي از زيرشبكه خارج شود هركدام از ساير مسيرياب‌هاي فعال احساس مي‌كنند از طريق ديگري مسيري بهتر به آن وجود دارد.

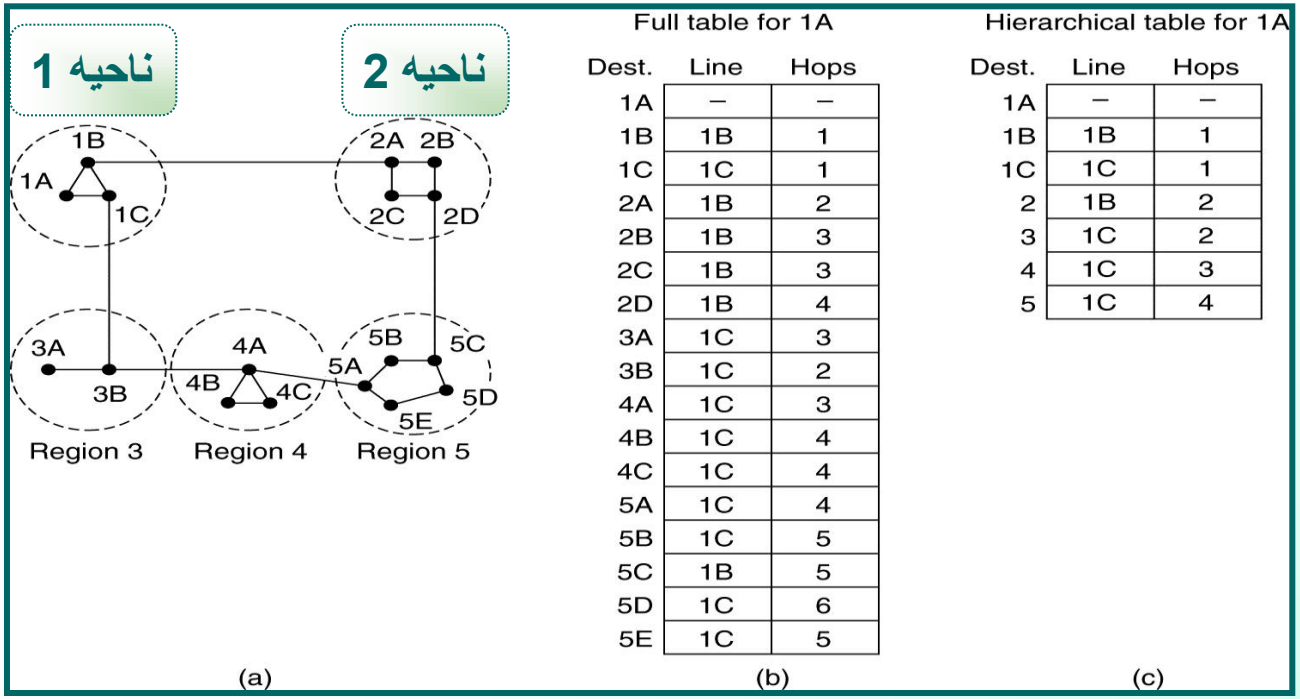


مسیریابی سلسله‌مراتبی Hierarchical Routing

رشد شبکه و زیادشدن شبکه‌هاي محلي و مسیریابها ، افزایش حجم جداول مسیریابي و زیادشدن زمان لازم جهت تعیین مسیر یك بسته و درنتیجه ایجاد تأخیرهاي بحراني و کاهش کارآیي شبکه

در مسیریابي سلسله‌مراتبي ، مسیریابها در گروههایي به نام "ناحیه Region" دسته‌بندي مي‌شوند. هر مسیریاب فقط "نواحي" و مسیریابهاي درون ناحیة خود را مي‌شناسد و هیچ اطلاعي از مسیریابهاي درون نواحي دیگر ندارد.

مسیریابی سلسله‌مراتبی



مشكل روش سلسله مراتبي

به دليل مشخص‌نبودن كل توپولوژي زيرشبكه براي هر مسيرياب :

ممكن است مسير انتخابي جهت ارسال بسته به يك مسيرياب خاص درون يك ناحيه بهينه نباشد.

مزيت استفاده از روشهای سلسله مراتبی: صرفه جويي در اندازه جداول مسيريابي

	تعداد ناحیه Regions	تعداد دسته Clusters	تعداد حوزه Zones	تعداد مسیریاب	تعداد رکورد در جدول
مسیریابی DV بدون سلسله‌مراتب	۱	–	–	۷۲۰	۷۲۰
مسیریابی DV با سلسله‌مراتب دوسطحی	۲۴	–	–	۳۰	۵۳
مسیریابی DV با سلسله‌مراتب سه‌سطحی	۹	۸	–	۱۰	۲۵
مسیریابی DV با سلسله‌مراتب سه‌سطحی	۹	۵	۴	۴	۱۹

مقایسه اندازه جدول مسیریابی در روشهای سلسله مراتبی

مسیریابی در اینترنت

اینترنت مجموعه‌اي از شبکه‌هاي خودمختار Autonomous و "مستقل" است که به نحوي به هم متصل شده‌اند.
شبکهٔ خودمختار که اختصاراً AS نامیده مي‌شود ، شبکه‌اي است که تحت نظارت و سرپرستي يك مجموعه يا سازمان خاص پياده و اداره مي‌شود. مثلاً يك دانشگاه

مسئول شبکهٔ خودمختار مي‌تواند بر روي شبکهٔ تحت نظارت خود "حاکميّت" داشته باشد يعني مي‌تواند بر روي تك‌تك اجزاي شبکه ، طراحي زيرساخت ارتباطي و طريقهٔ اتصال شبکه‌هاي محلي و نوع پروتکل ، سيستم عامل(ماشينهاي ميزبان) ، توپولوژي کل شبکه مسيريابي اعمال نفوذ کرده و نظرات خود را پياده نمايد.

مسیریابی در شبکه های خود مختار

مسیریابي بسته‌هاي IP در درون يك شبكة خودمختار بيشتر تابع پارامترهايي نظير سرعت و قابل اعتماد بودن الگوريتم مسيريابي است .

دروازه‌های مرزی Border Gateway:

مسيريابهايي كه ارتباط دو شبكة خودمختار متفاوت را برقرار مي‌كنند و تمامي ارتباطات بين‌شبكه‌اي از طريق آنها انجام مي‌شود .

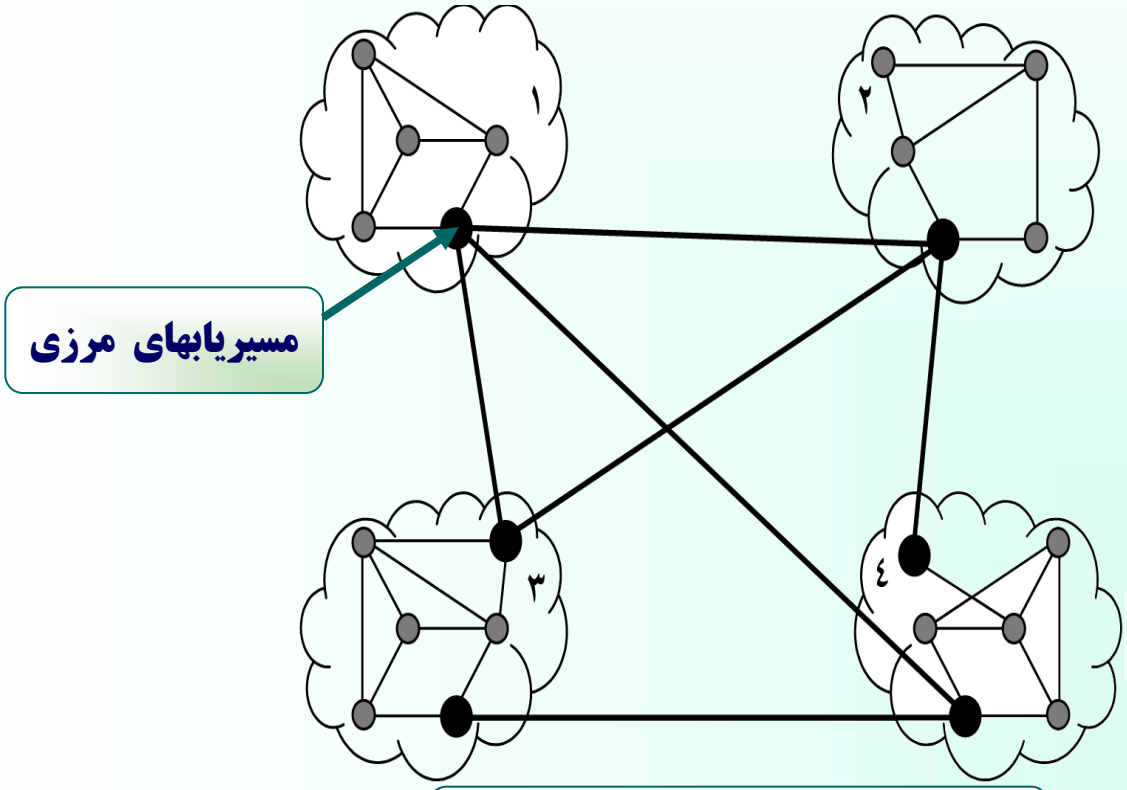
دروازه‌های مرزی Interior Gateway

مسيريابهايي كه ارتباط دو شبكة خودمختار متفاوت را برقرار مي‌كنند و تمامي ارتباطات بين‌شبكه‌اي از طريق آنها انجام مي‌شود.

- مسيريابهاي مرزي و ساختار ارتباطي بين آنها تابع قواعد "مسيريابي بروني"
- مسيريابهاي داخلي تابع الگوريتمهاي "مسيريابي دروني" مرزي
- مسيريابهاي مرزي = مسيريابهاي BGP

مثال: اگر يك ماشين ميزبان در شبكة 1 بخواهد بسته‌اي براي ماشين ديگر در شبكة 4 بفرستد سه مرحله مسيريابي لازم است:

- مسيريابي در درون شبكة 1 تا رسيدن بسته به مسيرياب مرزي
- مسيريابي روي خطوط ارتباطي بين‌شبكه‌اي تا رسيدن به شبكة 4
- مسيريابي درون شبكة 4 تا رسيدن به ماشين مقصد

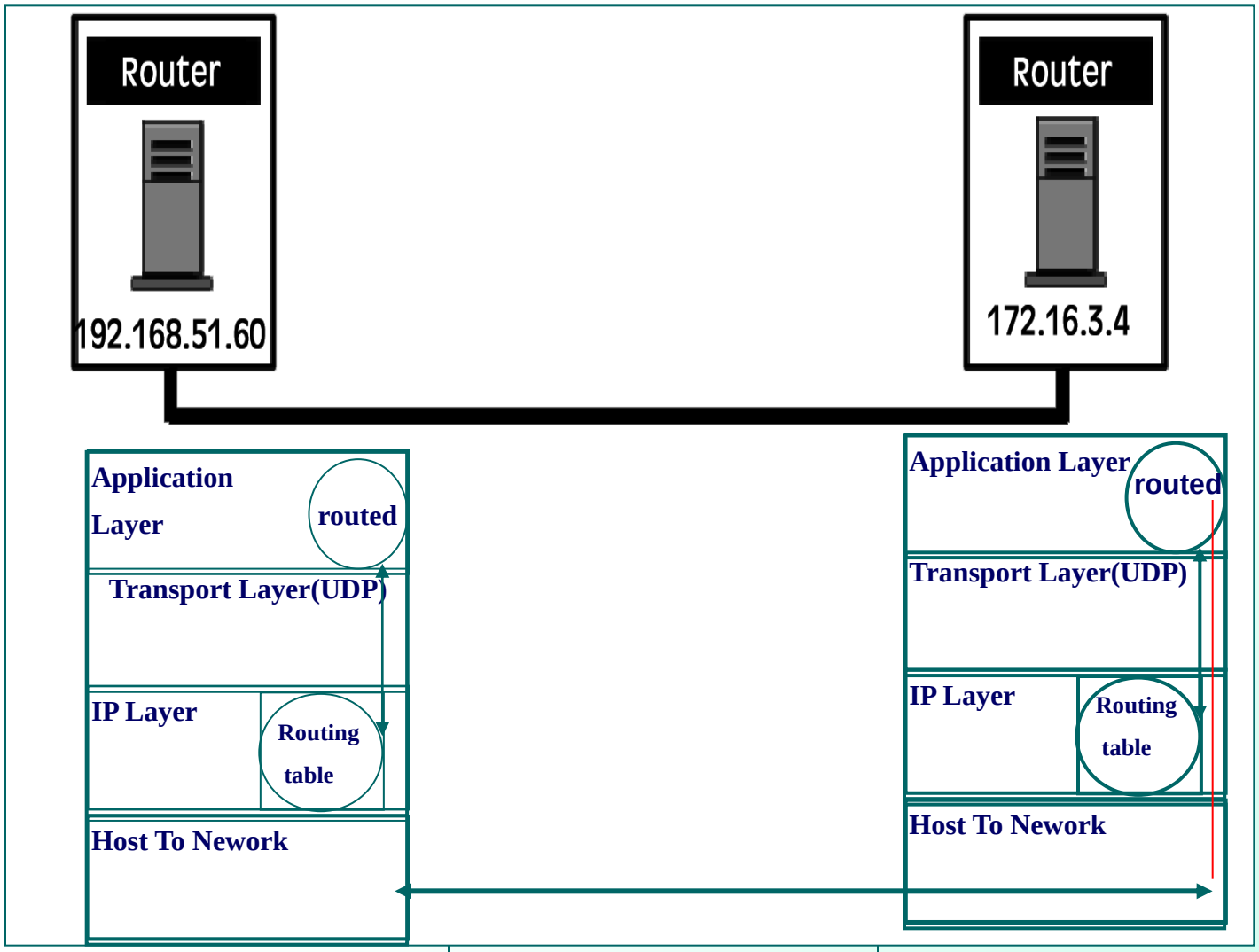


مثالی از چهار شبکهٔ AS متصل به هم

پروتکلRIP در مسیریابی درونی : Routing Information Protocol

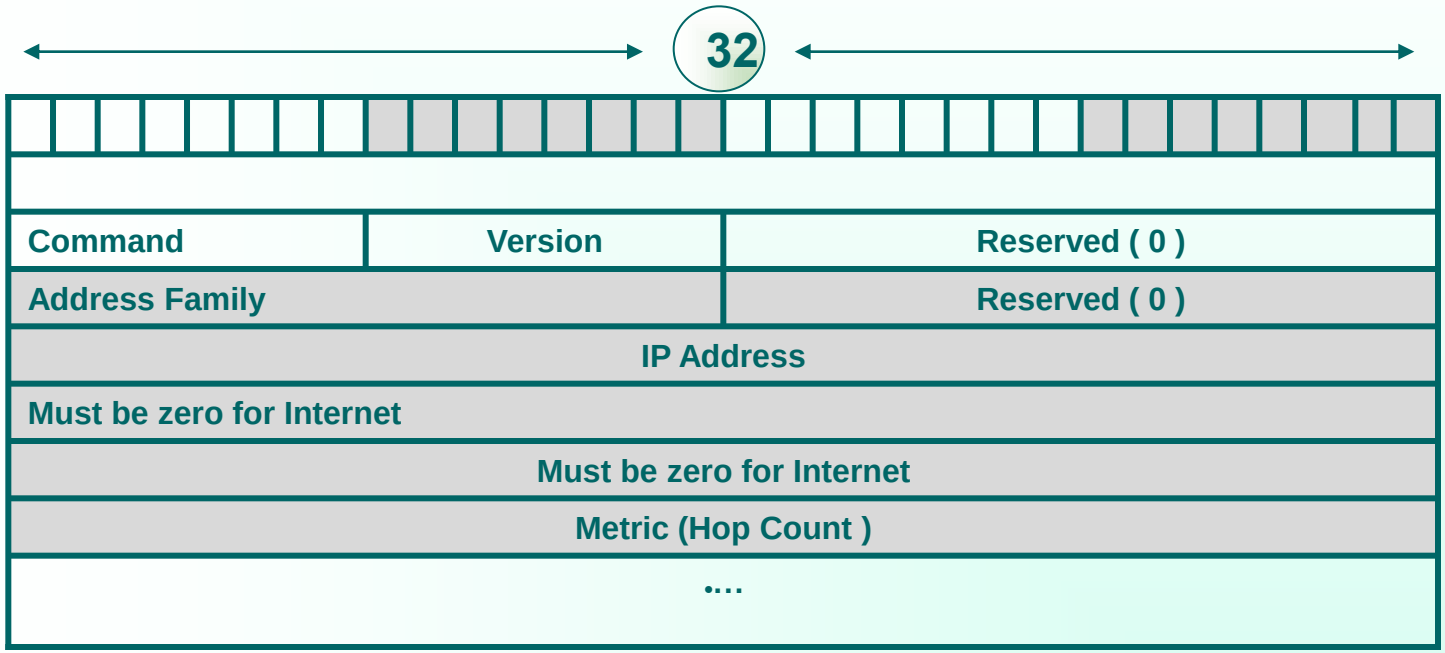
- اولين پروتكل مسيريابي دروني (1982)
- مبتني بر الگوريتم بردار فاصله DV
- معيار هزينه = تعداد گام
- مبادله جداول مسيريابي هر 30 ثانيه يكبار بين مسيريابهاي مجاور
- حداكثر تعداد طول مسير = 15
- استفاده از پروتكل UDP و پورت شماره 250 جهت مبادله جداول مسيريابي

جداول مسيريابي در لايه دوم جهت مسيريابي بسته‌هاي IP
مبادله جداول و عمليات به هنگام‌سازي توسط برنامه كاربردي لايه چهارم



پروتكل RIP در لاية كاربرد

قالب پیامها در پروتکل RIP



پروتکل OSPF در مسیریابی درونی Open Shortest Path First

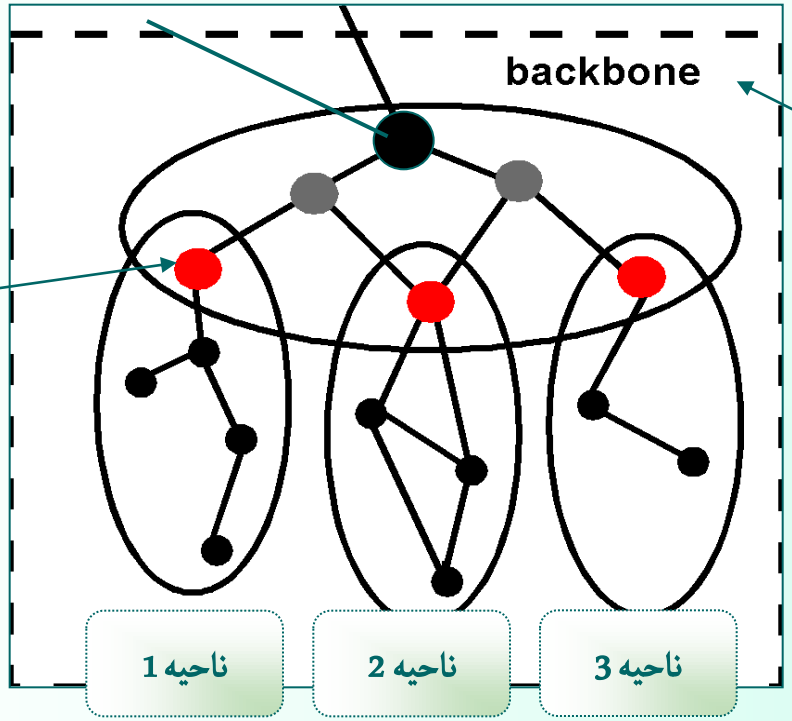
مقایسه پروتکل OSPF با RIP

- استفاده از الگوریتم LS براي محاسبة بهترين مسير بر خلاف پروتكل RIP و عدم وجود مشكل "شمارش تا بينهايت"
- توانايي در نظر گرفتن چندين معيار هزينه در انتخاب بهترين مسير برخلاف پروتكل RIP
- در نظرگرفتن حجم بار و ترافيك يك مسيرياب در محاسبة بهترين مسير بر خلاف پروتكل RIP و همگرايي سريع جداول مسيريابي در هنگام خرابي يك مسيرياب
- انتخاب مسير مناسب براي يك بسته بر اساس نوع سرويس درخواستي با توجه به فيلد Type of Service در بستة IP بر خلاف پروتكل RIP

مقايسه پروتكل OSPF با RIP

- هدايت نكردن تمام بسته‌هاي ارسالي براي يك مقصد خاص ، روي بهترين مسير و ارسال درصدي از بسته‌ها روي مسيرهاي در رتبه 2و 3 و ... از نظر هزينه ، بر خلاف پروتكل RIP = موازنه = Load Balancing
- پشتيباني از مسيريابي سلسله‌مراتبي برخلاف پروتكل RIP
- عدم قبول جداول مسيريابي مسيريابها توسط هر مسيرياب بدون احراز هويت ارسال‌كنندة آن
- استفاده مستقيم از پروتكل IP برخلاف پروتكل RIP (استفاده از پروتكل UDP در لايه انتقال)

- تقسيم يك شبكه خود مختار به تعدادي ناحيه و اطلاع تمام مسيريابهاي درون يك ناحيه از مسيريابهاي هم ناحيه و هزينه ارتباط بين آنها و ذخيره آن در جدول
- ارسال جداول براي تمام مسيريابهاي هم ناحيه در زمانهاي بهنگام‌سازي



مجموعه مسیریابهای مرزی +
سیریابهای خارج از هر ناحیه +
ساختار ارتباطی بین این مسیریابها

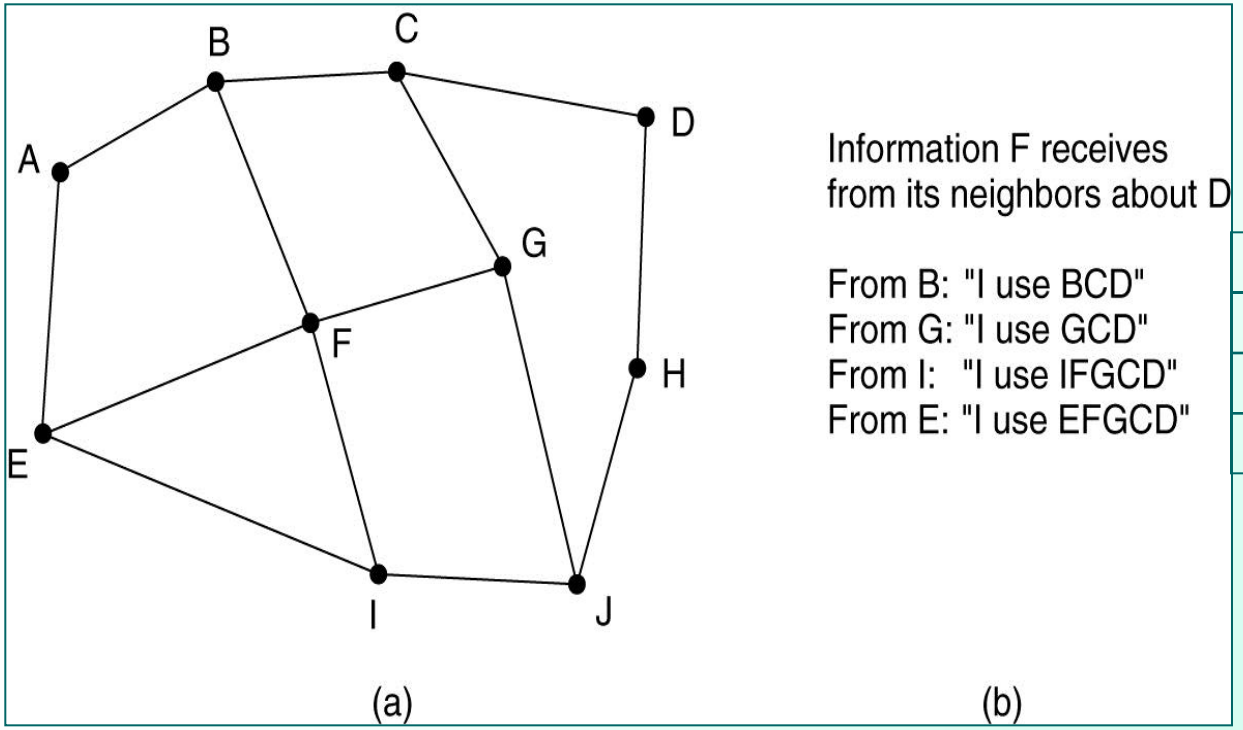
مسیریابهای مرزی
برقرارکننده ارتباط نواحی

سلسله‌مراتب مسیریابی در پروتکل OSPF

پروتکل BGP : پروتکل مسیریابی برونی The Exterior Gateway Routing Protocol

- الگوريتمهاي مسيريابي بين شبكه‌هاي خود مختار در اينترنت : BGP
- به جاي مبادله جداول مسيريابي و هزينه‌ها در پروتكل BGP بين مسيريابهاي مجاور ، ارسال فهرستي از مسيرهاي كامل بين هر دو مسيرياب در شبكه براي مسيريابهاي مجاور در بازه‌هاي زماني T ثانيه‌اي (بدون تعيين هزينه)

دریافت اطلاعات توسط مسیریاب F در مورد مسیریاب D از مسیریابهای مجاور



تعیین مسیر رسیده از B

تعیین مسیر رسیده از G

تعیین مسیر رسیده از I

تعیین مسیر رسیده از B

ساختار فرضي از ارتباط بين مسيريابهاي BGP

الگوريتمهائي كه در تبادل اطلاعات با همسايگان مسيرهاي كامل را به اطلاع يكديگر مي‌رسانند:

اولاً: مشكل "شمارش تا بينهايت" را نخواهد داشت. مانند پروتكل **BGP**

ثانياً: مسيريابهاي ديگر مي‌توانند بر روي كل مسير ، بررسي‌هاي امنيتي ، اقتصادي ، سياسي و ملي انجام دهند و بر اساس اين پارامترها مسير مناسب را انتخاب نمايند. مانند پروتكل **BGP**

تبادل اطلاعات مسيريابي (فهرست مسيرها) در پروتكل **BGP** در قالب پيام

انواع پيام تعريف شده در پروتكل **BGP**:

1. پيام **OPEN**
2. پيام **KEEPALIVE**
3. پيام **NOTIFICATION**
4. پيام **UPDATE**

فصل سوم : لایه انتقال در شبکه اینترنت

هدفهای آموزشی :

- مفاهیم لایه انتقال
- مفهوم پورت و سوکت
- تشریح پروتکل TCP
- روش برقراري ارتباط در پروتکل TCP
- روش کنترل جریان داده‌ها در پروتکل TCP
- زمان سنجها و عملکرد آنها در پروتکل TCP
- پروتکل UDP


پروتکلهای لایه انتقال
UDP
User Datagram Protocol
TCP
Transmisson Control Protocol

لايه IP

- هدايت و مسيريابي بسته‌هاي اطلاعاتي از يک ماشين ميزبان به ماشين ديگر
- عدم حل مشکلات احتمالي به وجود آمده براي بسته‌هاي IP در مسير

لايه انتقال

- فراهم آوردن خدمات سازماندهي‌شده, مبتني بر اصول سيستم عامل, براي برنامه‌هاي کاربردي در لايه بالاتر
- جبران کاستي‌هاي لايه IP

کاستی‌های لایه IP

- عدم تضمین درآماده‌بودن ماشین مقصد جهت دریافت بسته

O عدم تضمین در به ترتیب رسیدن بسته‌هاي متوالي و داده‌ها و صحت آنها

راهکارهای پروتکلTCP

- برقراري یک ارتباط و اقدام به هماهنگي بین مبدأ و مقصد قبل از ارسال هر گونه داده

O قراردادن شماره ترتیب براي داده‌ها

O تنظیم کد 16 بیتي کشف خطا در مبدأ و بررسي مجدد آن در مقصد جهت اطمینان از صحت داده‌ها

کاستی‌های لایه IP

❖ عدم تمایز در دریافت بسته‌هاي تکراري در مقصد (Duplication Problem)

➢ عدم تنظیم سرعت ارسال و تحویل بسته‌ها

❑ عدم توزیع بسته‌ها بین پروسه‌هاي مختلف اجرا شده بر روي یک ماشین واحد

راهکارهای پروتکل TCP

❖ قرار دادن شماره ترتیب در بسته ارسالي

➢ استفاده از الگوریتم پویا جهت تنظیم مجموعه زمانسنجها

❑ قراردادن آدرس پورت پروسه فرستنده و گیرنده در سرآیند بسته ارسالي

آدرس پورت

شماره شناسايي مشخص‌كننده هر پروسه براي برقراري يک ارتباط با پروسه‌ي ديگر بر روي شبکه

شماره پورتهای استاندارد

Port	Protocol	Use
21	FTP	File transfer
23	Telnet	Remote login
25	SMTP	E-mail
69	TFTP	Trivial File Transfer Protocol
79	Finger	Lookup info about a user
80	HTTP	World Wide Web
110	POP-3	Remote e-mail access
119	NNTP	USENET news

آدرس سوکت

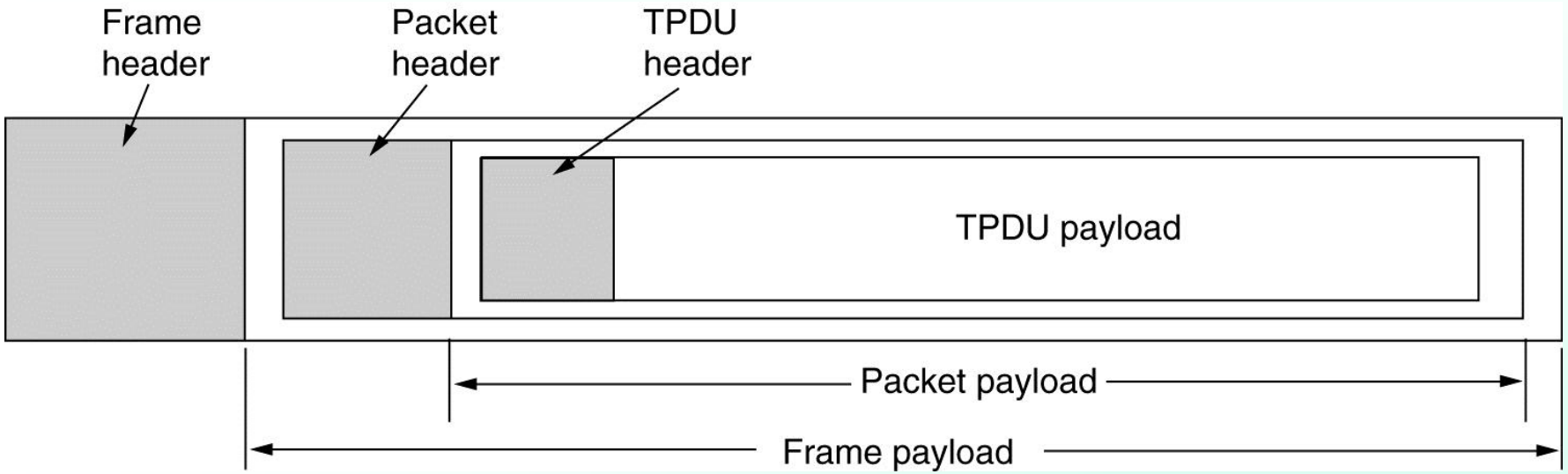
زوج آدرس IP و آدرس پورت مشخص‌کننده یک پروسه یکتا و واحد بر روي هر ماشین در دنیا

(IP Address: Port Number)= Socket Address

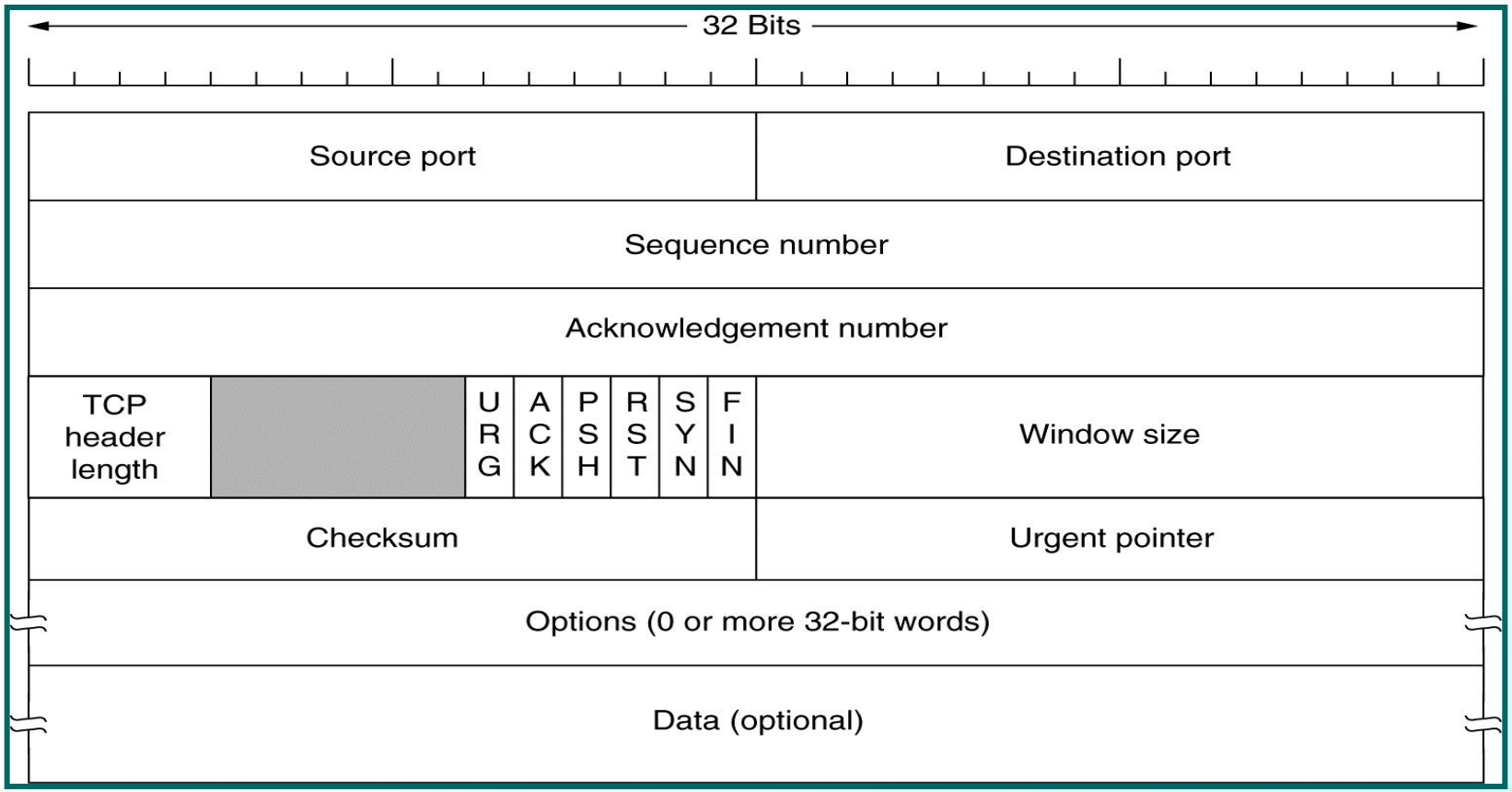
مثال 80 : 193.142.22.121

ساختار بسته های پروتکل TCP

TPDU = Transport Protocol Data Unit= بسته تولید شده در لایه انتقال = قطعهTCP



بسته پروتکل TCP



فیلد Source Port

- فیلد 16بیتي
- آدرس پورت پروسه مبدأ

فیلد Destination Port

- فیلد 16 بیتي
- آدرس پورت پروسه مقصد

فیلد Sequence Number

- فیلد 32 بیتي
- مشخص کننده شماره ترتیب آخرین بایت قرارگرفته شده در فیلد داده از بسته جاري

فیلد Acknowledgement Number

- فیلد 32 بیتي
- مشخص‌کننده شماره ترتیب بایتي که فرستنده بسته منتظر دریافت آن است

فیلد TCP Header Lenght

- فیلد 4 بیتي
- مشخص کننده طول سرآیند بسته TCP برمبناي کلمات 32 بیتي
- حداقل مقدار = 5
- تعیین کننده محل شروع داده‌ها در بسته TCP

۶ بیت بلااستفاده

6 بیت بلااستفاده جهت استفاده درآینده

بیتهای Flag

۶ بیتی

URG	ACK	PSH	RST	SYN	FIN

بیت URG

مقدار فیلد = 1 نشان دهنده معتبر بودن مقدار موجود در فیلد Urgent Pointer

مقدار فیلد = 0 نشان دهنده نا معتبربودن مقدار موجود در فیلد Urgent Pointer

U	A	P	R	S	F
R	C	S	S	Y	I
G	K	H	T	N	N

بیت ACK

مقدار فیلد = 1 نشان‌دهنده معتبر بودن مقدار موجود در فیلد
Acknowledgement Number

بیت PSH (PUSH)

مقدار فیلد = 1 نشان‌دهنده تقاضاي فرستنده اطلاعات از گیرنده اطلاعات جهت بافرنکردن داده‌هاي موجود در بسته و تحویل سریع بسته به برنامه‌هاي کاربردي به منظور انجام پردازشهاي بعدي

بیت RST

مقدار فیلد = 1 نشان‌دهنده قطع ارتباط به صورت یکطرفه و ناهماهنگ

بیت SYN

تغییر مقدار این فیلد جهت برقراري ارتباط توسط ماشین

روند برقرای ارتباط TCP

الف) تنظیم بیتهاي ACK=0 و SYN=1 توسط شروع کننده ارتباط در یک بسته TCP بدون داده (تقاضاي برقراري ارتباط = Connection Request)

ب) تنظیم بیتهاي SYN=1 و ACK=1 در صورت قبول طرف دریافت‌کننده بسته تقاضاي برقراري ارتباط به برقراري ارتباط

بیت FIN

مشخص‌کننده قطع و پایان ارسال اطلاعات هنگام اتمام داده‌هاي ارسالي توسط طرفين با 1 نمودن مقدار اين بيت هنگام ارسال آخرين بسته

قطع كامل ارتباط: 1 نمودن مقدار اين فيلد توسط هر دو ماشين فرستنده و گيرنده

قطع ارتباط يكطرفه: 1 نمودن مقدار اين فيلد توسط يكي از طرفين ارتباط

فیلد Windows Size

مشخص كننده مقدار ظرفيت خالي فضاي بافر گيرنده

فیلد Checksum

- فیلد 16 بیتي
- حاوي کد کشف خطا

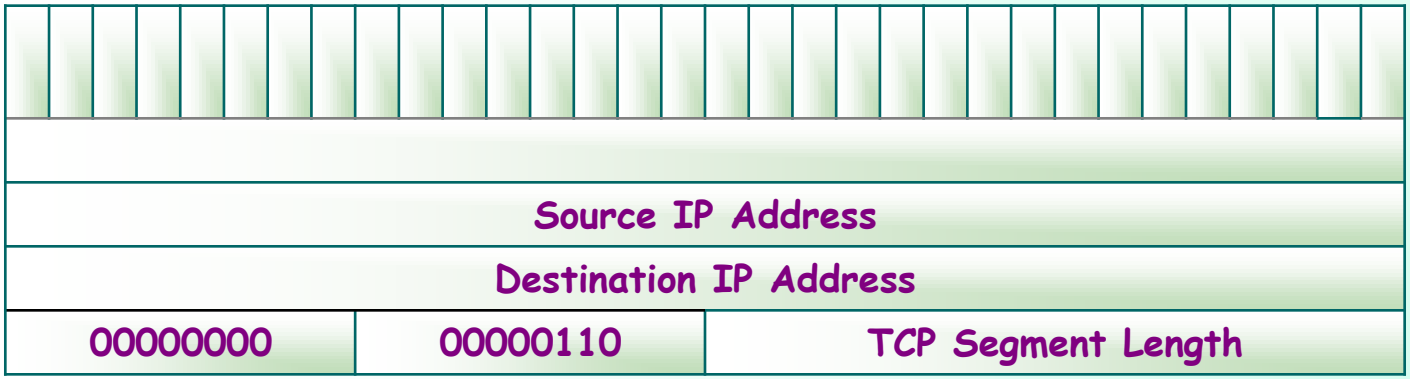
طریقه محاسبه کد کشف خطا

- تقسیم کل بسته TCP به قالبهاي 16 بیتي (منهاي قسمت Checksum)
- ایجاد یک سرآیند فرضي و تقسیم آن به صورت کلمات 16 بیتي
- جمع تمامي کلمات در مبناي مکمل 1 و منفي نمودن عدد حاصل در مبناي مکمل 1 و قرارگرفتن عدد حاصل در فیلد Checksum

جمع کل کلمات 16 بیتي موجود در بسته TCP + سرآیند فرضي = 0 عدم بروز خطا در حین ارسال داده‌ها

ساختار سرآیند فرضی

- 32 بیت آدرس IP ماشین مبدأ
- 32 بیت آدرس IP ماشین مقصد
- یک فیلد 8 بیتي کاملاً صفر
- فیلد 8 بیتي پروتکل که براي پروتکل TCP = 6
- فیلد TCP Segment Length = طول کل بسته TCP



فيلد Urgent Pointer

اشاره گر به موقعيت داده‌هاي اضطراري موجود در بسته TCP

فيلد Option

- فيلد اختياري
- شامل مقدار حداكثر طول بسته
- قراردادن كدهاي بي ارزش در اين فيلد به جهت آنكه طول بسته ضريبي از 4 باقي بماند

روش برقراری ارتباط در پروتکل TCP

روش دست تکاني سه مرحله‌اي

مرحله اول:

- ارسالِ یک بسته TCP خالي از داده از طرف شروع‌کننده ارتباط با بیتهاي SYN=1 و ACK=0 و قراردادن عدد x درون فیلد شماره ترتیب

- اعلام شروع ترتیب داده‌هاي ارسالي از x+1 به ماشین طرف مقابل
- پیشگیري از مساوي بودن شماره ترتیب داده‌هاي ارسالي با انتخاب مقدار X به صورت تصادفي

روش دست تكاني سه مرحله‌اي

مرحله دوم :

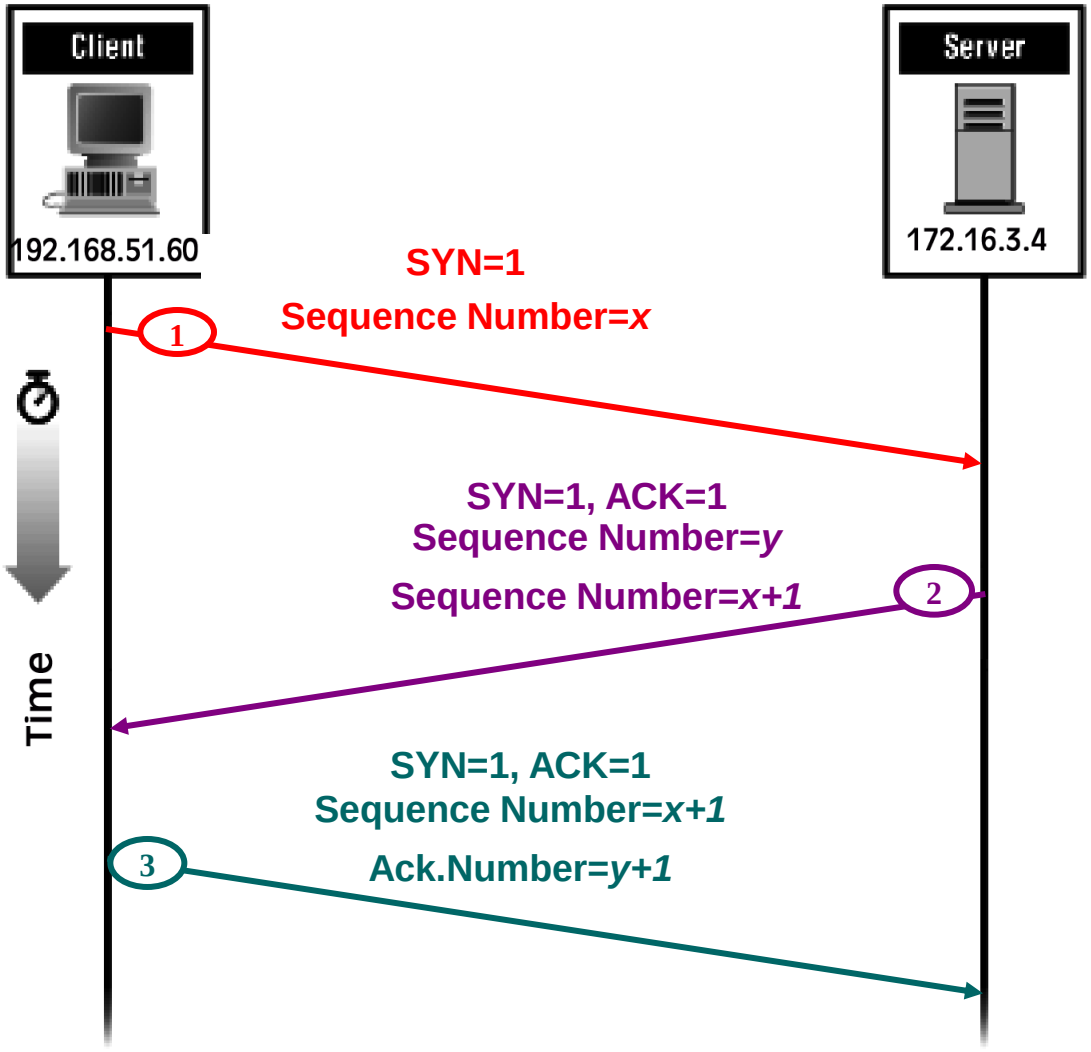
- **رد تقاضاي برقراري ارتباط:** ارسال بسته‌اي خالي با بيت **RST=1**
- **قبول تقاضاي برقراري ارتباط:** ارسال بسته خالي با مشخصات زير از طرف گيرنده بسته تقاضا:
  - بيت **SYN = 1**
  - بيت **ACK = 1**
  - **Acknowledgement = x+1**
  - **Sequence Number = y**

روش دست تكاني سه مرحله‌اي

مرحله سوم:

تصديق شروع ارتباط از طرف شروع‌كننده ارتباط با قراردادن مقادير زير در بيتهاي:

- SYN = 1
- ACK = 1
- Acknowledgement Number = y + 1
- Seq. No = x + 1



مراحل دست تکانی سه مرحله ای برای برقراری ارتباط در پروتکلTCP

روند خاتمه ارتباط TCP

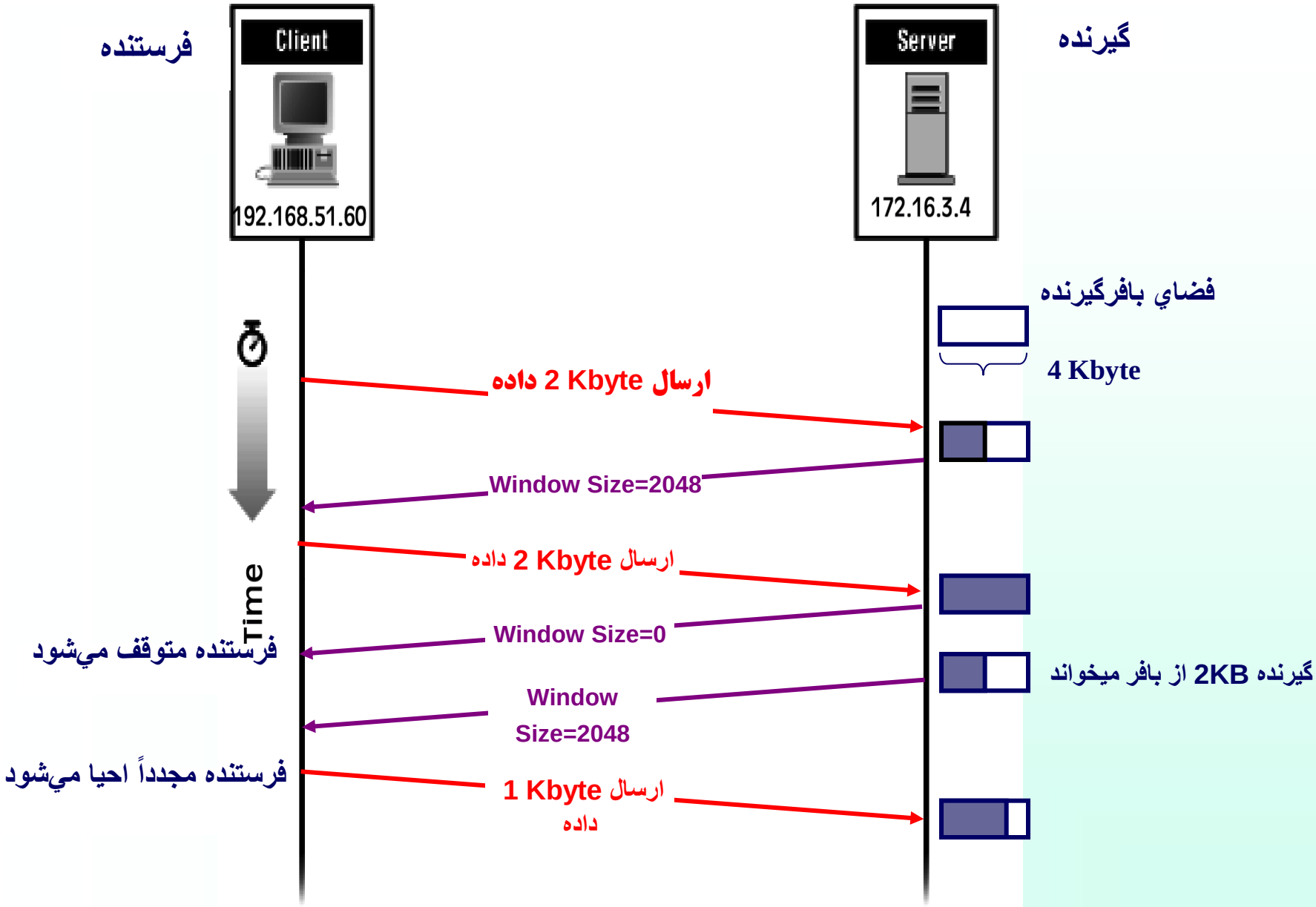
- ارسال بسته TCP با بیت FIN = 1 از طرف درخواست‌کننده اتمام ارسال
- موافقت طرف مقابل با اتمام ارتباط یکطرفه و ادامه ارسال داده توسط آن
- قطع ارتباط دو طرفه با یک نمودن مقدار بیت FIN در آخرین بسته ارسالي و تصدیق پایان ارتباط از طرف مقابل

کنترل جریان در پروتکل TCP

- استفاده از بافر جهت کنترل جریان داده‌ها در پروتکل TCP
- بافرشدن داده‌ها قبل از ارسال به برنامه کاربردي لايه بالاتر
- امکان عدم دریافت و ذخیره داده‌ها توسط برنامه کاربردي درمهلت مقرر و پرشدن بافر اعلام حجم فضاي آزاد بافر در فیلد Window درهنگام ارسال بسته TCP به طرف مقابل
- ایجاد یک ساختمان داده خاص به ازاي هر ارتباط برقرارشده TCP و نگهداري اطلاعاتي ازآخرين وضعيت ارسال و دريافت جریان داده‌ها = ساختمان داده بلوک نظارت بر انتقال = TCB = Transmission Control Block

نام متغير	توضيح
متغيرهای نظارت بر ارسال داده‌ها	
SND.UNA	شمارة ترتيب آخرين بسته اي كه ارسال شده ولي هنوز پيغام Ack آن برنگشته است.
SND.NXT	شمارة ترتيب آخرين بايت كه داده ها از آن شماره به بعد در بستة بعدي كه بايد ارسال شود.
SND.WND	ميزان فضاي آزاد در بافر ارسال
SND.UP	شمارة ترتيب آخرين داده هاي اضطراري كه تحويل برنامة كاربردي شده است.
SND .WL1	
SND.WL2	
SND.PUSH	شمارة ترتيب آخرين داده هايي كه بايد آني به برنامة كاربردي گسيل (Push) شود.
SND.ISS	مقدار اولية شمارندة ترتيب داده هاي دريافتي كه در حين ارتباط بر روي آن توافق مي‌شود.
متغيرهای نظارت بر دريافت داده‌ها	
RCV.NXT	شمارة ترتيب آخرين بايت در بستة بعدي كه از آن شماره به بعد انتظار دريافت آنرا دارد.
RCV.WND	ميزان فضاي آزاد در بافر دريافت
RCV.UP	شمارة ترتيب آخرين داده هاي اضطراري كه براي برنامة طرف مقابل ارسال شده است.
RCV.IRS	مقدار اولية شمارندة ترتيب داده هاي ارسالي كه در حين ارتباط بر روي آن توافق مي‌شود.

متغيرهاي ساختمان داده TCP



مثال روند کنترل جریان در پروتکل TCP

زمان سنجها در پروتکل TCP

TCP Timer

وابستگي عملكرد صحيح پروتكل **TCP** به استفاده درست از زمان سنجها

زمان سنجها

- ❑ Retransmission Timer
- ❑ Keep- Alive Timer
- ❑ Persistence Timer
- ❑ Quite Timer
- ❑ Idle Timer

زمان سنج Retransmission Timer

پس از برقراري ارتباط و ارسال بسته براي پروسه مقصد, زمان‌سنجي (RT) با مقدار پيش فرض تنظيم و فعال مي‌گردد و شروع به شمارش معكوس مي‌نمايد كه اگر در مهلت مقرر پيغام دريافت بسته (Ack) نرسيد رخداد انقضاي زمان تكرار روي داده و ارسال مجدد بسته صورت گيرد.

عملکرد این زمان سنج Retransmission Timer بسیار ساده است اما مشکل در اینجاست که:

1- عمل ارسال مجدد یک بسته چند بار باید تکرارشود ؟

2- مقدار پیش فرض زمان سنج چه مقدار باشد ؟

بهترین راه تنظیم زمان سنج : روشهاي وفقي و پويا

الف) ایجاد یک متغیر حافظه یه نام RTT و مقداردهي آن هنگام برقراري یک ارتباط TCP

ب) تنظیم یک زمان‌سنج به ازاي ارسال هر بسته و اندازه زمان رفت و برگشت پیغام دریافت بسته = M

الگوریتم Jacobson

ج) بهنگام شدن مقدار پیش فرض زمان سنج از رابطه:

$$RTT_{new}=RTT_{old}+4*D_{new}$$

$$D_{new}=\alpha.D_{old}+(1-\alpha).(RTT_{old}-M)$$

$$\alpha=7/8$$

مقدار اولیه D مي‌تواند صفر باشد.

Keep- Alive Timer

- توقف ارسال اطلاعات و عدم تبادل داده علي رغم فعال و باز بودن ارتباط TCP
- قطع ارتباط يكي از طرفين به دليل خرابي سخت افزاري و يا نرم افزاري

جهت تمايز اين دو حالت

ارسال بسته TCP خالي از داده از طرف فرستنده اطلاعات براي مقصد با استفاده از زمان سنج Keep-Alive Timer (زمان پيش فرض بين 5 تا 45 ثانيه)

عدم بازگشت پيغام دريافت

قطع ارتباط به صورت يكطرفه و آزاد نمودن تمام بافرها

بازگشت پيغام دريافت از طرف مقصد

ارتباط TCP باز و فعال است

- مقدار فضاي بافر آزاد يكي از طرفين ارتباط صفر (Window Size= 0) متوقف شدن پروسه طرف مقابل
- خالي شدن مقداري از فضاي بافر پر شده بعد از مدتي اعلام آزادشدن فضاي بافر جهت احياي پروسه بلوكه و متوقف شده توسط سيستم عامل و شروع و ادامه ارسال پروسه متوقف شده

Persistence Timer

ارسال بسته TCP در فواصل زماني منظم با استفاده از زمان سنج Persistence Timer پس از آزاد شدن فضاي بافر براي پروسه بلوكه‌شده جهت احيا و ادامه ارسال داده توسط آن

Quite Timer

هنگام بسته شدن يک ارتباط TCP با شماره پورت خاص تا مدت زمان معيني که زمان سنج Quite Timer تعيين مي نمايد (مقدار پيش فرض = 30 تا 120 ثانيه) هيچ پروسه اي اجازه استفاده از شماره پورت بسته شده را ندارد.

جهت رسيدن بسته هاي سرگردان ناشي از ارتباط پايان يافته موجود در شبکه به مقصد

Idle Timer

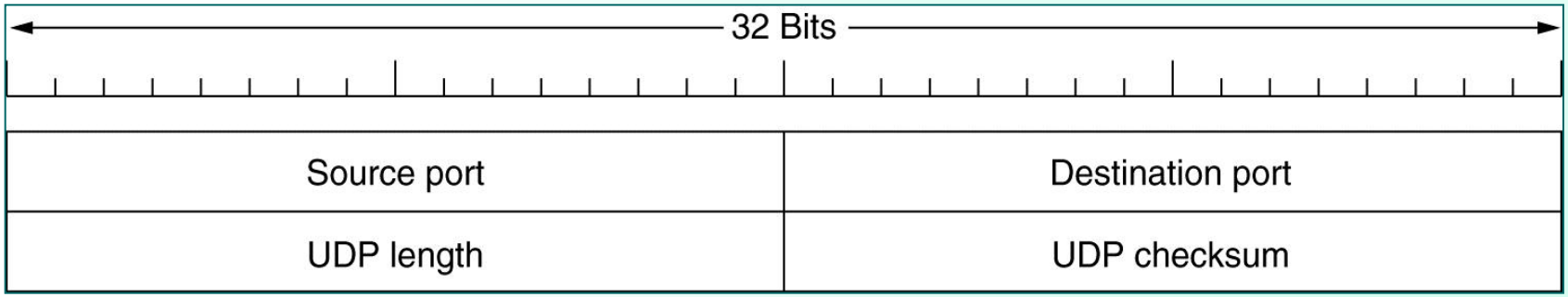
اگر تلاش براي تکرار ارسال يک بسته بيش از حد متعارف انجام شود ارتباط TCP را بصورت يکطرفه رها کرده و قطع مي‌نمايد. مقدارمعمول آن 360 ثانيه است.

پروتکل UDP

- پروتکل بدون اتصال (Connectionless)
- پروتکل ساده و سریع
- کاربرد در سیستم هاي DNS و TFTP

ارسال بسته به مقصد بدون اطمینان ازبرقراري ارتباط و آماده بودن ماشین مقصد

بسته UDP



فیلدهای بسته UDP

فیلد Source Port

- فیلد 16 بیتی
- مشخص کننده آدرس پورت پروسه مبدأ

فیلد Detination Port

- فیلد 16 بیتی
- مشخص‌کننده آدرس پورت پروسه مقصد

فیلد UDP Length

- فیلد 16 بیتی
- طول بسته UDP بر حسب بایت (شامل سرآیند و داده‌ها)

فیلد UDP Checksum

- فیلد 16 بیتي
- درج کد کشف خطا در این فیلد
- فیلد اختیاري (جهت ارسال دیجیتال صدا و تصویر مقدار تمام بیتها صفر)

مناسبترین کاربرد پروتکل **UDP** = پروسه هایي که عملیات آنها مبتني بریک تقاضا و یک پاسخ مي‌باشد.

مانند : سیستم **DNS**

ماشینهای Big Edition و Little Edition

ماشين‌هاي **Big Endian** : ماشين‌هايي كه ابتدا بايت پرارزش و سپس بايت كم ارزش را ذخيره مي‌كنند مثل كامپيوترهاي سري **SUN**

ماشين‌هاي **little Endian** : ماشين‌هايي كه ابتدا بايت كم ارزش و سپس بايت پرارزش را ذخيره مي‌كنند مثل كامپيوترهاي شخصي با پردازنده سري **80X86** و پنتيوم

تشکیل بسته‌هاي IP ابتدا در حافظه و ارسال از طریق سخت افزار شبکه دریافت بسته IP ارسالي از یک ماشین Big Endian به یک ماشین Little Endian و یا برعکس تعویض بایتها و فاقد ارزش بودن محتوي بسته دریافتي

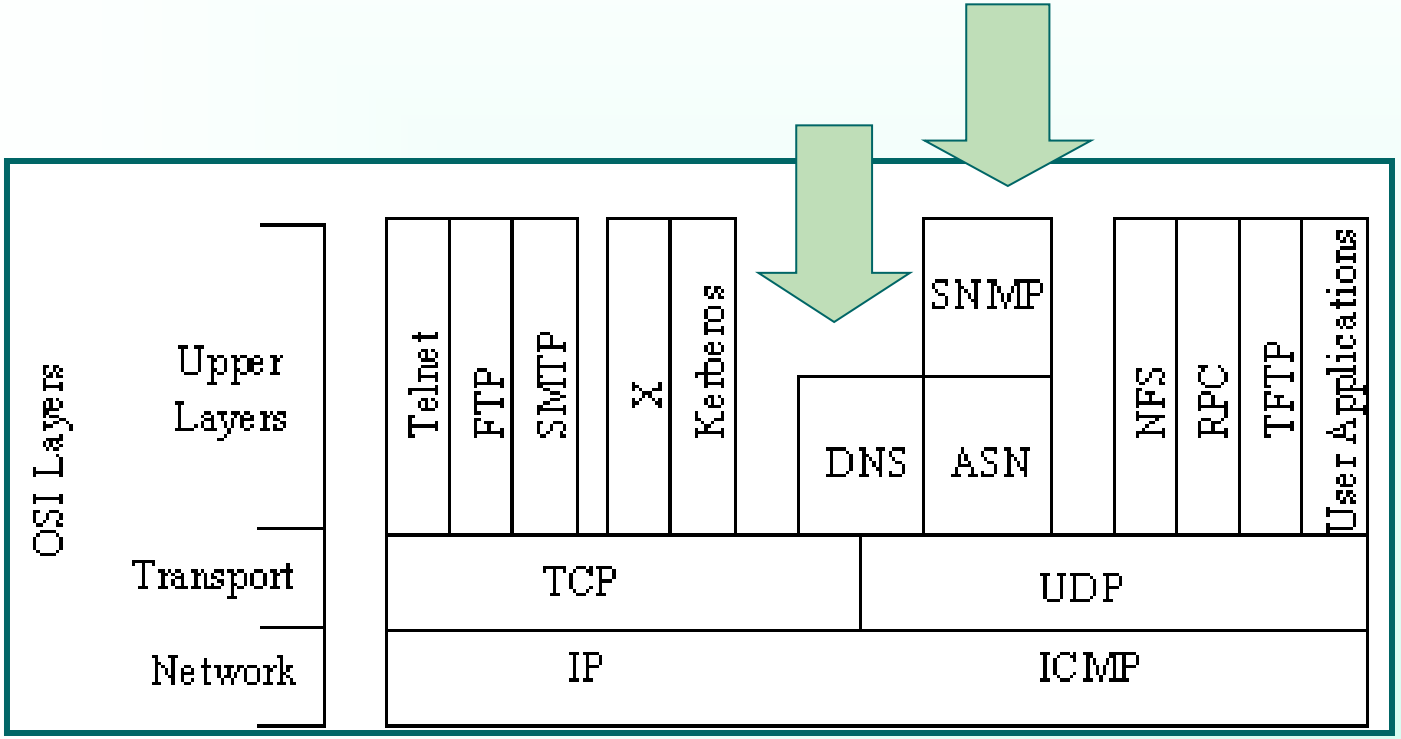
پروتکل TCP/IP ، استاندارد ماشین‌هاي Big Endian را مبنا قرار داده است

فصل چهارم: سرویس دهنده‌های نام حوزه DNS و اصول مدیریت شبکه SNMP

هدفهای آموزشی :

- اصول سرویس دهنده‌هاي نام
- مفهوم نام حوزه و سلسله مراتب نام
- روشهاي جستجو در سرویس دهنده‌هاي نام
  - پرس‌وجوي تکراري
  - پرس‌وجوي بازگشتي
  - پرس‌وجوي معکوس
- ساختار بانک اطلاعاتي در سرویس دهنده‌هاي نام
- قالب پیام در سرویس‌دهنده‌هاي نام حوزه
- اصول مدیریت شبکه در اینترنت
- اصول پروتکل SNMP

SNMP و DNS


OSI Layers
Upper Layers
Transport
Network
Telnet
FTP
SMTP
X
Kerberos
SNMP
DNS
ASN
NFS
RPC
TFTP
User Applications
TCP
UDP
IP
ICMP

سرویس دهنده نامهای حوزه (Domain Name System)

آدرسها در دنياي واقعي = آدرسهاي اينترنت = آدرسهاي نمادين = نام حوزه

مانند: www.ibm.com

ترجمه آدرسهای نمادین به آدرسهای IP

۱) روش متمرکز: - تعريف تمام نامها و آدرسهاي IP معادل در يک فايل به نام hosts.txt

- استفاده از فايل hosts.txt جهت ترجمه يک نام نمادين به آدرس IP معادل آن توسط تابع مترجم نام موجود در هر ماشين ميزبان

کاربرد در شبکه ARPANET

و شبکه هاي کوچک و داخلي

2) DNS يا سيستم نامگذاري حوزه:

- روشي سلسله مراتبي
- توزيع بانک اطلاعاتي مربوط به نامهاي نمادين و معادل IP آنها در کل شبکه اينترنت
- معرفي اين سيستم در سال 1984
- کاربرد در شبکه‌هاي بزرگ مانند اينترنت

روش ترجمه نام در DNS

- فراخواني تابع تحليلگر نام Name Resolver توسط برنامه کاربردي
- پارامتر ورودي تابع تحليلگر نام آدرس نمادين
- ارسال بسته UDP (بسته درخواست) به آدرس يک سرويس‌دهنده DNS (به صورت پيش فرض مشخص مي باشد) توسط تابع
- تحويل آدرس IP معادل با آدرس نمادين از طرف سرويس‌دهنده به تابع تحليلگر
- تحويل آدرس IP به برنامه کاربردي درخواست‌کننده

نام حوزه

- تشکیل نام حوزه از بخشهايي به نام سطح
- تفکیک سطحها در نام حوزه با علامت •
- اشاره هر سطح از نام حوزه به یک قسمت از بانک اطلاعاتي توزیع شده
- تحلیل یک نام حوزه از سطوح سمت راست به چپ جهت پیدا نمودن سرویس‌دهنده متناظر

مثال : www.yahoo.com

www.president.ir

هفت حوزه عمومی

.Com

موسسات اقتصادي و تجاري

commercial

.edu

موسسات علمي يا دانشگاهي

educational

.net

ارائه دهندگان خدمات شبکه

Network Service provider

.int

سازمانهاي بين المللي

international

.gov

آژانسهاي دولتي آمريکا

government

.mil

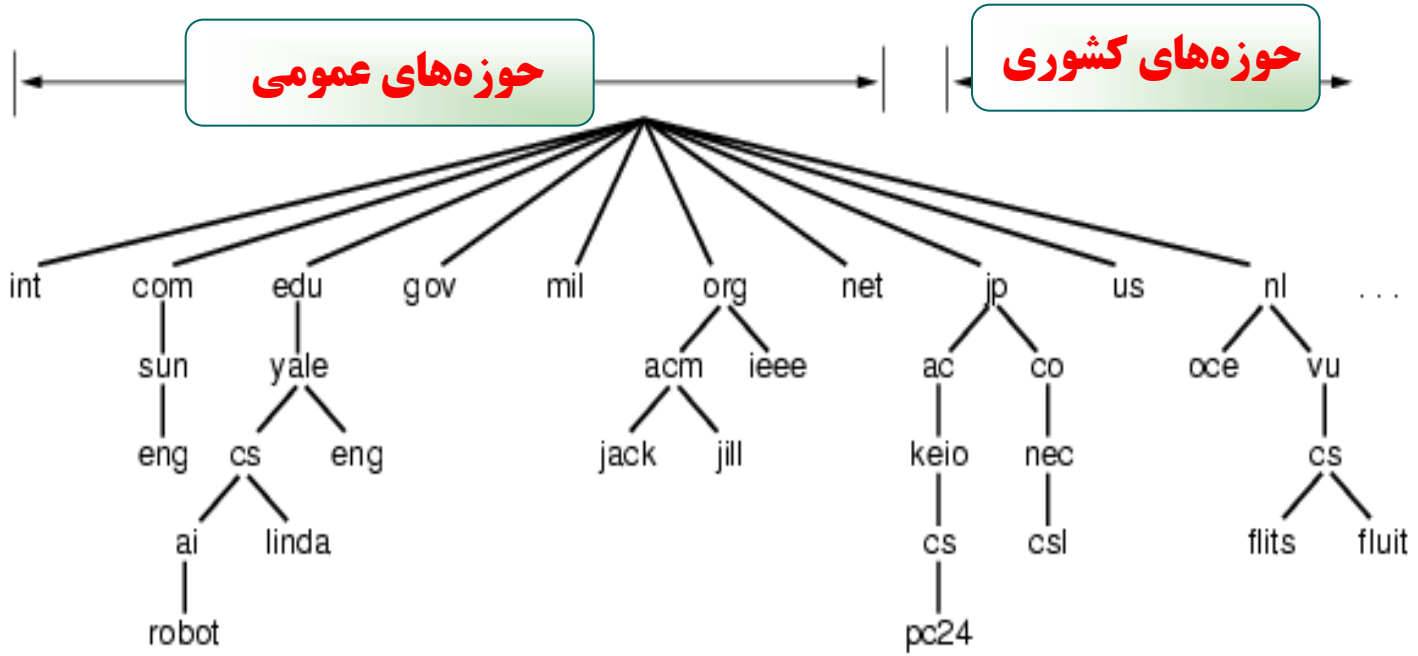
سازمانهاي نظامي دنيا

military

.org

سازمانهاي غير انتفاعي

organization



حوزه‌های عمومی و حوزه‌های کشوری

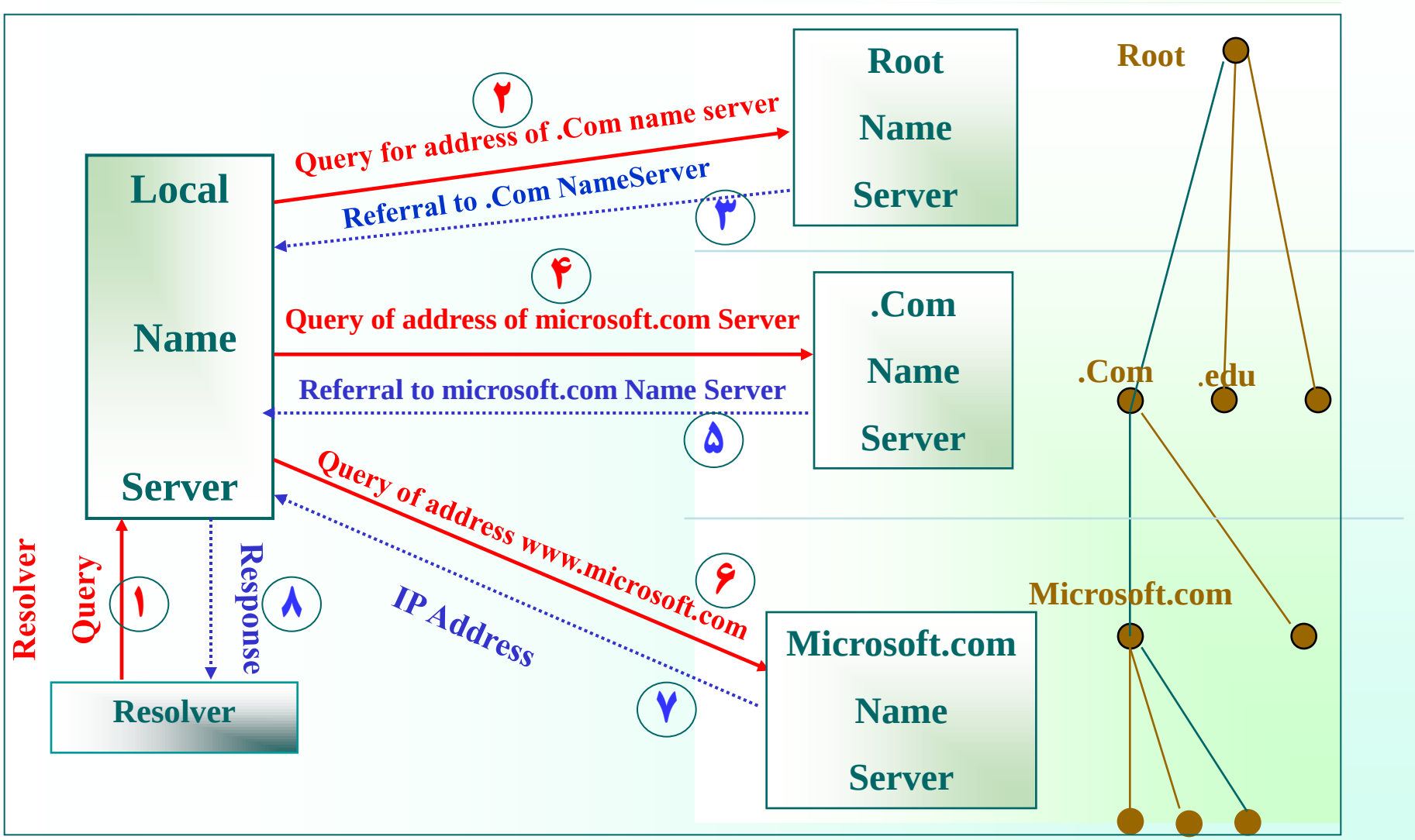
روشهای جستجو در سرویس دهنده‌های نام

- پرس‌وجوي تكراري — Iterative Query
- پرس‌وجوي بازگشتي — Recursive Query
- پرس‌وجوي معكوس — Reverse Query

پرس و جوی تکراری

- حجم عمده عملیات بر عهده سرویس‌دهنده محلي
- داشتن آدرس ماشین Root به عنوان نقطه شروع توسط سرویس‌دهنده محلي
- ترجمه نام به آدرس IP بعد از دریافت تقاضاي تبدیل نام توسط سرویس دهنده محلي و ارسال آن به تقاضا کننده در صورت امکان
- در غیر این صورت ارسال یک تقاضا براي DNS سطح بالا جهت ترجمه نام
- معرفي آدرس ماشین دیگر به سرویس دهنده محلي جهت ترجمه نام مورد نظر توسط سرویس‌دهنده سطح بالا
- ارسال تقاضا از طرف سرویس‌دهنده محلي به سرویس‌دهنده معرفي شده در مرحله قبل
- ترجمه نام حوزه توسط سرویس‌دهنده نام در غیر این صورت برگرداندن آدرس سرویس دهنده سطح پایین تر به سرویس‌دهنده محلي
- ادامه این روند تا ترجمه نام حوزه به آدرس IP توسط DNS نهایي

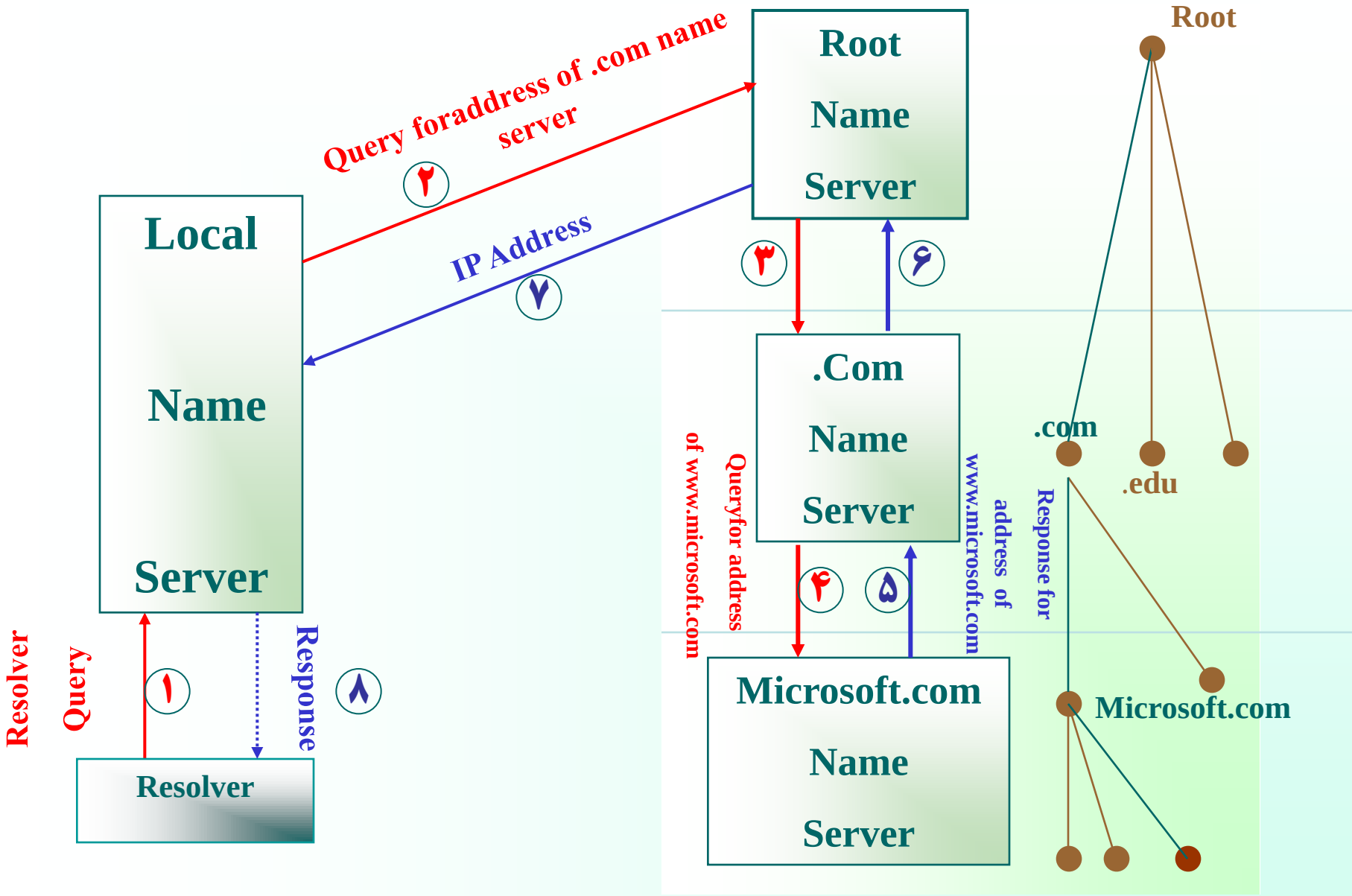
ترجمه نام www.microsoft.com به روش پرس و جوی تکراری



پرس و جوی بازگشتی

- ارسال تقاضاي تبديل نام به روش UDP به سرويس‌دهنده محلي از طرف تابع سيستمي تحليل نام
- برگرداندن مقدار معادل IP در صورت موجودبودن در بانك اطلاعاتي مربوط به سرويس‌دهنده محلي
- در صورت نبود معادل IP نام حوزه در بانك اطلاعاتي سرويس‌دهنده محلي ، ارسال تقاضاي ترجمه آدرس توسط خود سرويس‌دهنده به سرويس دهنده سطح بالاتر
- پيگيري ترجمه آدرس به همين ترتيب توسط سرويس‌دهنده‌هاي سطوح مختلف و به دست آوردن آدرس IP معادل

در روش پرس‌وجوي بازگشتي ماشين سرويس‌دهندة محلي اين مراحل متوالي را نمي‌بيند و هيچ كاري جز ارسال تقاضاي ترجمة يك آدرس برعهده ندارد و پس از ارسال تقاضا براي سرويس‌دهندة سطح بالا منتظر خواهد ماند.



ترجمه نام www.microsoft.com به روش پرس و جوی بازگشتی

پرس و جوی معکوس

- داشتن آدرس IP يك ماشين و نياز به پيدا كردن نام نمادين معادل با آن توسط سرويس‌دهنده DNS
- انجام يك جستجوي وقت‌گير و كامل جهت پيدا نمودن نام نمادين

روش كار:

- ارسال يك تقاضا توسط سرويس‌دهنده محلي براي DNS متناظر با شبكه‌اي كه مشخصه آن در آدرس IP موجود است .
- ارسال تقاضاي مربوطه توسط DNS مربوط به شبكه به سرويس‌دهنده‌هاي متناظر با هر زير شبكه
- برگرداندن نام نمادين حوزه معادل با آدرس IP

ساختار بانک اطلاعاتی سرویس دهنده‌های نام

پروسه سرویس‌دهنده

- برنامة اجرايي جهت پردازش تقاضاهاي ترجمة نام از ماشينهاي ديگر و ارسال پاسخ مناسب براي تقاضادهنده
- استانداردبودن قالب هر تقاضا در شبکة اينترنت جهت ارسال تقاضا و دريافت پاسخ توسط هر ماشين فارغ از ساختار و سيستم عامل آن

بانک اطلاعاتی

- ذخیره داده‌هاي لازم براي تحليل يك نام نمادين در بانك اطلاعاتي
- يكسان نبودن ساختار بانك اطلاعاتي در سرويس‌دهنده‌هاي گوناگون
- بانك اطلاعاتي = بانك ركوردهاي منبع = فايل RR = Resource Records

فايل RR

- نگهداري در حافظة اصلي جهت بالابردن سرعت جستجو
- فايل متني
- در نظرگرفتن زمان اعتبار براي هر ركورد درون فايل

نمونه‌های ساختا ر کوردهای فایل RR

Domain Name	Time to live	Class	Type	Value

Domain Name	Type	Class	Time to Live	Length	Value

Domain Name

مشخص‌کننده نام حوزه یا نام مربوط به يك ماشين (نام نمادين)

Time to Live

نشان دهنده مدت اعتبار رکورد (بر حسب ثانیه)

مقدار فیلد معمولاً 86400 ثانیه

Class

اين فيلد مشخص مي‌كند كه ماهيّت نام نمادين مربوط به چه شبكه‌اي است

كلاس IN رکورد مربوط به يك نام در شبكة اينترنت

كلاس CHAOS

كلاس Hesiod

Type

مشخص‌کننده نوع رکورد

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

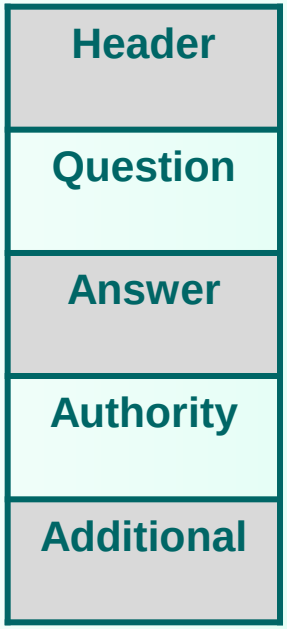
انواع رکوردهاي اصلي در بانك اطلاعاتي DNS

```
;Authoritative  data for  cs.vu.nl
cs.vu.nl.  86400 IN SOA  star boss (952771,7200,2419200,86400)
cs.vu.nl.  86400 IN TXT  “Faculteit wiskunde en informatica”
cs.vu.nl.  86400 IN TXT  “Virje universiteit Amsteradam”
cs.vu.nl.  86400 IN MX    1 zephyr.cs.vu.nl.
cs.vu.nl.  86400 IN MX    2 top .cs.vu.nl.

flits.cs vu.nl.     86400  IN HINFO    SUN  UNIX
flits.cs vu.nl.     86400  IN  A          130.37.231.165
flits.cs vu.nl.     86400  IN  A          192.31.231.165
flits.cs vu.nl.     86400  IN  MX       1 flits.cs.vu.nl
flits.cs vu.nl.     86400  IN MX        2 zephyr .cs.vu.nl
flits.cs vu.nl.     86400  IN  MX       3 top.cs.vu.nl
www.cs.vu.nl.  86400  IN CNAME  star.cs.vu.nl
ftp.cs.vu.nl.      86400  IN CNAME  zephyr.cs. vy.nl

rowboat                  IN    A          130.37.56.201
                         IN    MX       1 rowboat
                         IN    MX        2 zephyr

little-sister              IN     A          130.37.62.23
                           IN     HINFO  Mac MacOS

laserjet                  IN        A         192.31.231.216
                          IN       HINFO  “HP LaserJet IIISi Proprietary”
```

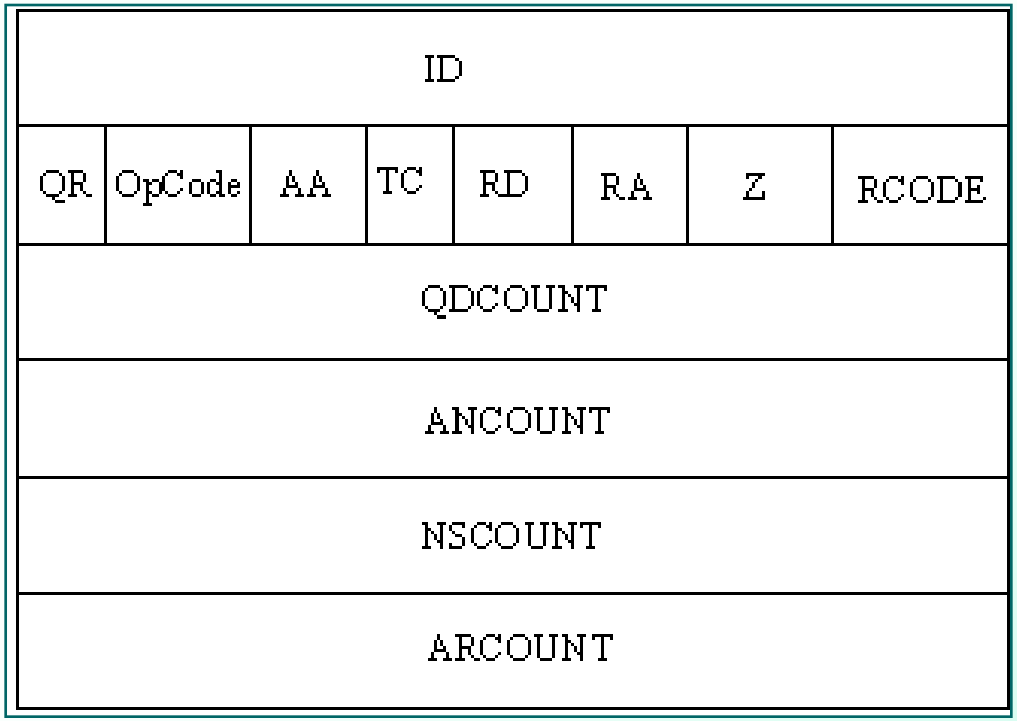
نمونه فایل RR در یک سرویس‌دهندهٔ نام

قالب پیامهای پرس وجو در سرویس‌دهنده‌های نام

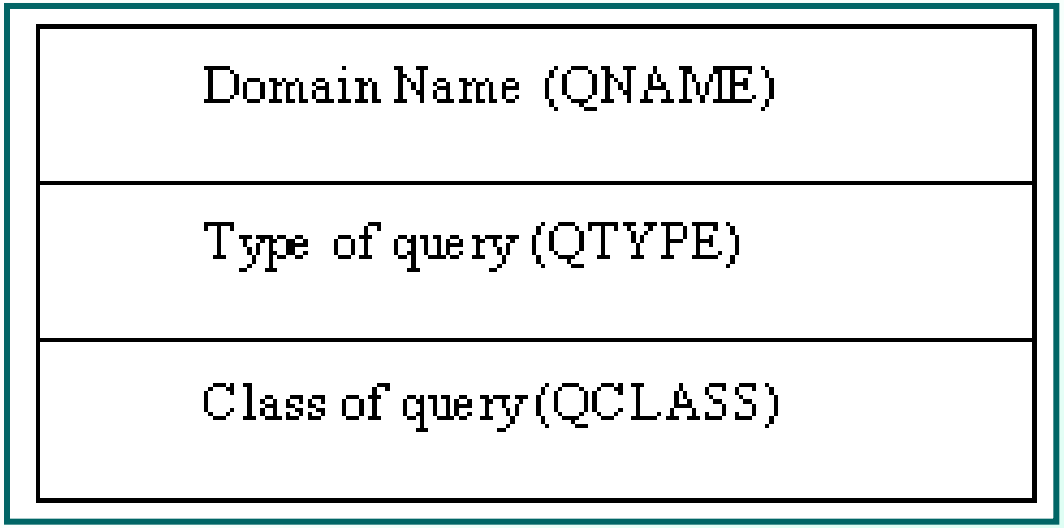
- بخش سرآیند پیام
- بخش پرسش
- خش پاسخ
- بخش اطلاعات ناحیه
- بخش اطلاعات اضافي



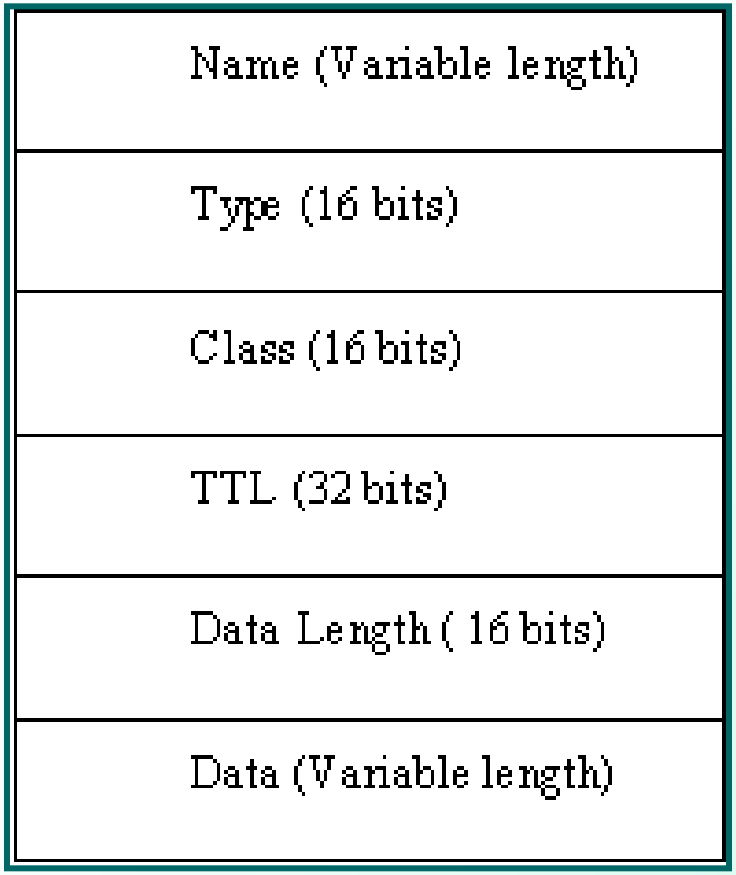
فیلدهای بخش سر آیند پیام



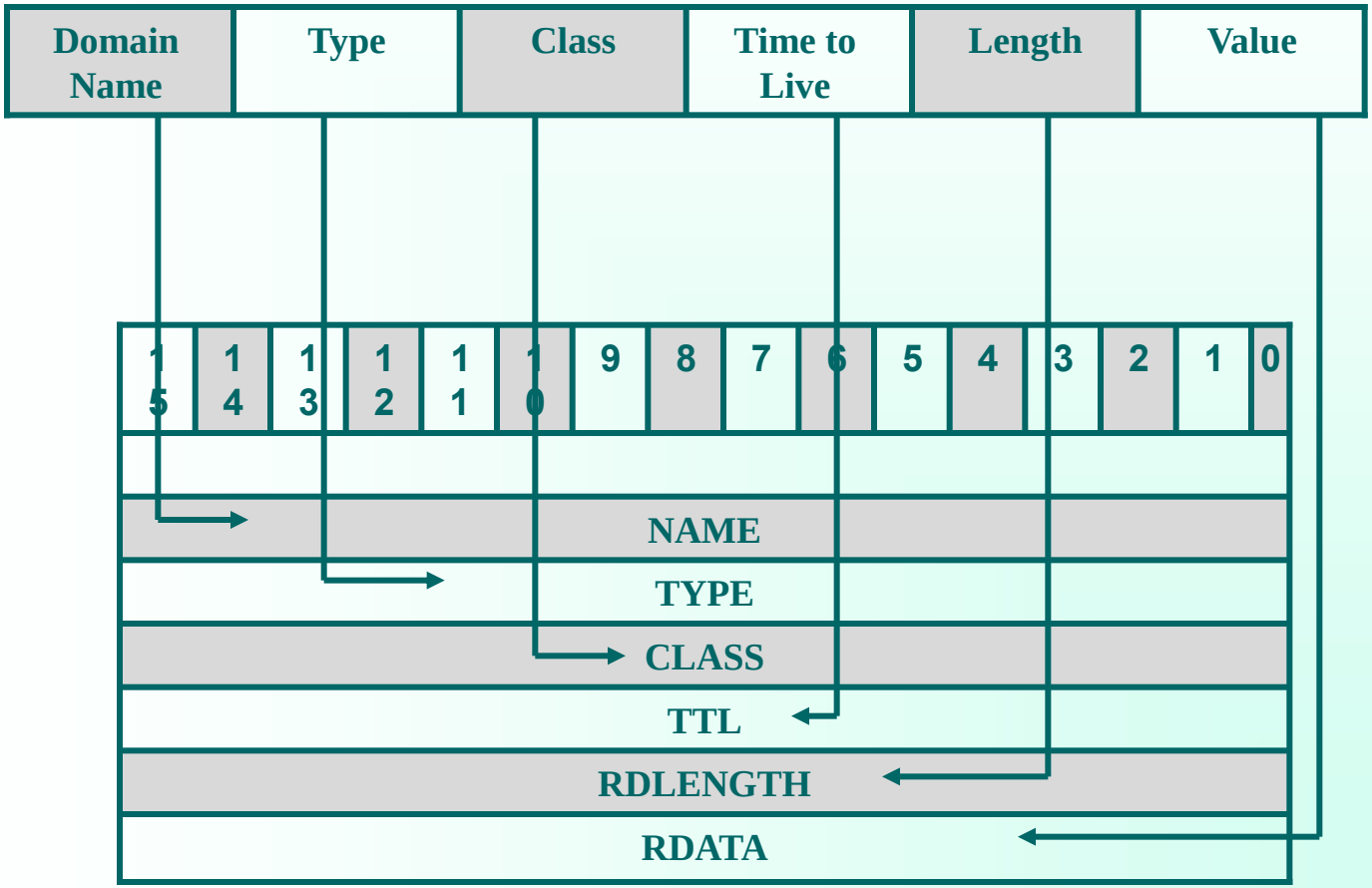
فیلدهای بخش پرسش پیام



فیلدهای بخش پاسخ ، اطلاعات ناحیه و بخش اطلاعات اضافی



نمونه جاسازی یک رکورد در یک پیام ارسالی از سرویس‌دهندهٔ نام



مقدمه‌ای بر مدیریت شبکه

لزوم بكارگيري پروتكلهاي شبكه

نظارت بر وضعيت شبكه و اجزاي آن و همچنين توانايي اعمال مديريت بر روي ماشينهاي ميزبان و اجزاي يك زيرشبكه (شامل مسيريابها ، پلها و ...)

توجه

پياده‌سازي نرم‌افزارهاي مديريت شبكه در لايه كاربرد جهت مستقل‌نمودن پروتكل‌هاي مديريت از سخت‌افزار شبكه

معماری پروتکلهای مدیریت شبکه

- تعریف استاندارد مبادله اطلاعات لازم براي نظارت و مدیریت بین ماشینها و مدیر شبکه
- تعریف استاندارد نظارت و کنترل و همچنین تعریف اطلاعات مدیریتي

استانداردهای مدیریت شبکه

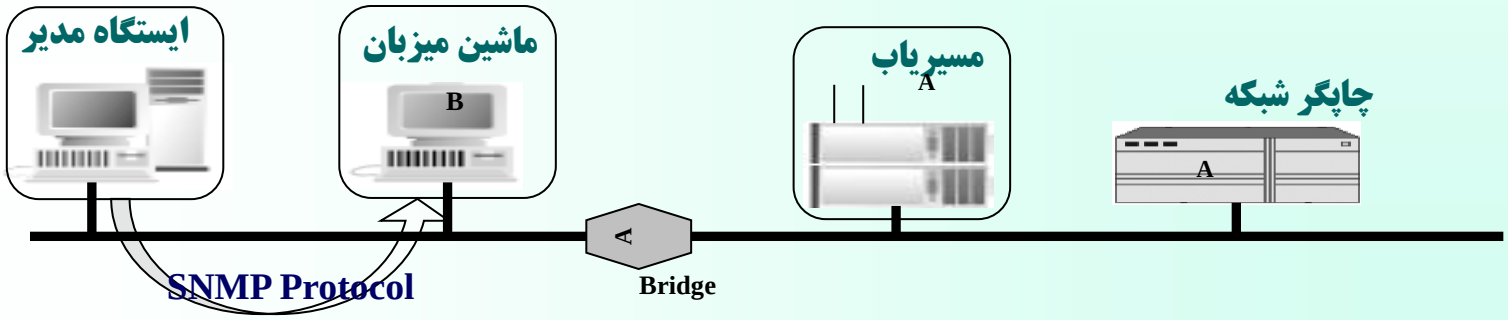
- CMOT
- RMON
- SNMPv

مدل SNMP

Simple Network Management Protocol

تقسيم عناصر يك شبكة خودمختار به چهار ردة:

1. نودهاي تحت مديريت
2. ايستگاههاي مديريت
3. اطلاعات مديريت
4. قرارداد مديريت



اجزای مدل مدیریت در SNMP

۱– نودهای تحت مدیریت

- شامل ماشينهاي ميزبان ، مسيريابها ، پلها ، چاپگرها و هر ماشيني كه بتواند اطلاعاتي از وضعيت خود ، به ايستگاههاي مدير ارسال نمايد و از فرامين آنها تبعيت كند.
- يك نود تحت مديريت بايد قادر به اجراي پروسة كاربردي SNMP باشد. در اين حالت به آن ايستگاه نمايندگي SNMP گفته مي‌شود.
- هر نود تحت مديريت ممكن است در كنترل چند ايستگاه مديريت باشد كه هر يك از اين ايستگاههاي مدير ، سطوح دسترسي متفاوتي به آن ايستگاه دارند .

۲- ایستگاههای مدیریت

- مراکز مدیریت شبکه
- کامپیوترهاي همه‌منظوره شامل نرم‌افزار لازم جهت مدیریت

۳- اطلاعات مدیریت

مشخص کننده وضعیت فعلي ایستگاه (توصیف وضعیت ایستگاه توسط متغیرهاي وضعیت در حافظه)

۴- قرارداد مدیریت

روشي استاندارد و مستقل جهت برقراري ارتباط ايستگاه مدير با نمايندگيها به منظور تقاضاي حالت اشياء (متغيرهاي وضعيت) و تغيير آنها در صورت لزوم

لزوم ايجاد استانداردهای مدیریت داده

وجود مجموعة استانداردي از متغيرها براي توصيف وضعيت هر نود تحت مديريت (از قبيل ميزان ترافيك ورودي و خروجي ، نرخ خرابي بسته‌هاي داده ، وضعيت اجزاي مرتبط و ...).

پایگاه دادهٔ اطلاعات مدیریتی Management Information Base

MIB = مجموعة اطلاعات مديريتي و ساختار پياده‌سازي آن

استاندارد MIB

- مستقل از پروتكلهاي مديريت شبكه
- امكان تغيير پروتكل مديريت ، بدون نياز به تغيير MIB
- شامل 10 گروه از اشياء

X ستفاده پروتكلهاي مديريت شبكه از اطلاعات مديريتي يكسان

Group	# Objects	Description
System	7	Name, location, and description of the equipment
Interfaces	23	Network interfaces and their measured traffic
AT	3	Address translation (deprecated)
IP	42	IP packet statistics
ICMP	26	Statistics about ICMP messages received
TCP	19	TCP algorithms, parameters, and statistics
UDP	6	UDP traffic statistics
EGP	20	Exterior gateway protocol traffic statistics
Transmission	0	Reserved for media-specific MIBs
SNMP	29	SNMP traffic statistics

گروههای اشیاء MIB-II در اینترنت

زبان توصیفی ASN.1

- استانداردي جهت تعريف متغيرهاي حالت و اشياء
- دو مجموعه استاندارد **ASN.1**:
  - يك نوع زبان توصيف اشياء كه توسط كاربر قابل استفاده است.
  - يك روش كدگذاري براي مبادلة اطلاعات بين ايستگاههايي كه از پروتكل **SNMP** پشتيباني مي‌كنند.

پروتکل ساده مدیریت شبکه (SNMP)

به دلیل وجود انواع مختلفي از دستورات در يك پروتكل مديريت شبكه و در نتيجه پيچيدگي زياد به جهت اضافه كردن دستورات جديد براي هر نوع عملياتي

↓

استفاده از روش واكشي تمامي عمليات و فرمانها و ذخيره متغيرهاي حالت در پروتكل SNMP

Message	Description
Get-request	Requests the value of one or more variables
Get-next-request	Requests the variable following this one
Get-bulk-request	Fetches a large table
Set-request	Updates one or more variables
Inform-request	Manager-to-manager message describing local MIB
SnmpV2-trap	Agent-to-manager trap report

انواع پیغامهای SNMP

بخشهای پیغام SNMP

1. شماره نسخة پروتكل SNMP
2. يك شناسه كه گروه ايستگاههاي تحت نظارت يك مدير را مشخص مي‌كند.
3. بخش داده كه به چند واحد داده تقسيم مي‌شود.

```
SNMP-Message ::=
                SEQUENCE {
                    version INTEGER {
                                version-1 (0)
                    },
                community
                    OCTET STRING,
                data
                    ANY
                }
```

قالب پيغام به زبان ASN

فصل پنجم: برنامه‌نویسی تحت شبکه اینترنت

Socket Programming

هدفهای آموزشی :

- انواع سوکت و مفاهیم آنها
- مفهوم سرویس‌هنده /مشتري
- توابع مورد استفاده در برنامه سرویس‌دهنده
- توابع مورد استفاده در برنامه مشتري
- معرفي زبان جاوا
- آشنايي با اپلت

روال برقراری ارتباط بین دو برنامه از راه دور:

الف) درخواست برقراري ارتباط با كامپيوتري خاص با IP مشخص و برنامه‌اي روي آن كامپيوتر با آدرس پورت مشخص = درخواست فراخواني تابع سيستمي socket()

ب) مبادله داده‌ها با توابع send() و recv() در صورت برقراري ارتباط

ج) اتمام ارتباط با فراخواني تابع close()

انواع سوكت و مفاهيم آنها

- سوكتهاي نوع استريم = سوكتهاي اتصال گرا Connection Oriented
- سوكتهاي نوع ديتاگرام = سوكتهاي بدون اتصال Connectionless

سوكتهاي نوع استريم مبتني بر پروتكل TCP	لزوم برقراري يك اتصال قبل از مبادله داده‌ها به روش دست‌تكاني سه‌مرحله‌اي
سوكتهاي نوع ديتاگرام مبتني بر پروتكل UDP	مبادله داده بدون نياز به برقراري هيچ ارتباط و يا اتصالي و عدم تضميني

بررسيدن داده‌ها ، صحت داده‌ها و ترتيب داده‌ها

سوکتهای نوع استریم

کاربرد:

پروتکل انتقال فایل FTP

پروتکل انتقال صفحات ابرمتن HTTP

پروتکل انتقال نامه هاي الکترونيکي SMTP

سوکتهای نوع دیتاگرام

کاربرد:

انتقال صدا و و تصویر یا سیستم DNS

سوکت socket

- سوكت يك مفهوم انتزاعي از تعريف ارتباط در سطح برنامه‌نويسي
- اعلام آمادگي جهت مبادله داده‌ها نوسط برنامه‌نويس به سيستم عامل بدون درگير شدن با جزئيات پروتكل TCP يا UDP و تقاضاي ايجاد فضا و منابع مورد نياز جهت برقراري يك ارتباط از سيستم‌عامل

سرویس دهنده / مشتری

تعریف عمومی:

مشتري (client) : پروسه ایست نیازمند اطلاعات

سرویس دهنده (server):

پروسه اي است براي به اشتراك گذاشتن اطلاعات و تحویل اطلاعات به مشتري

برنامه سمت سرویس دهنده Server Side

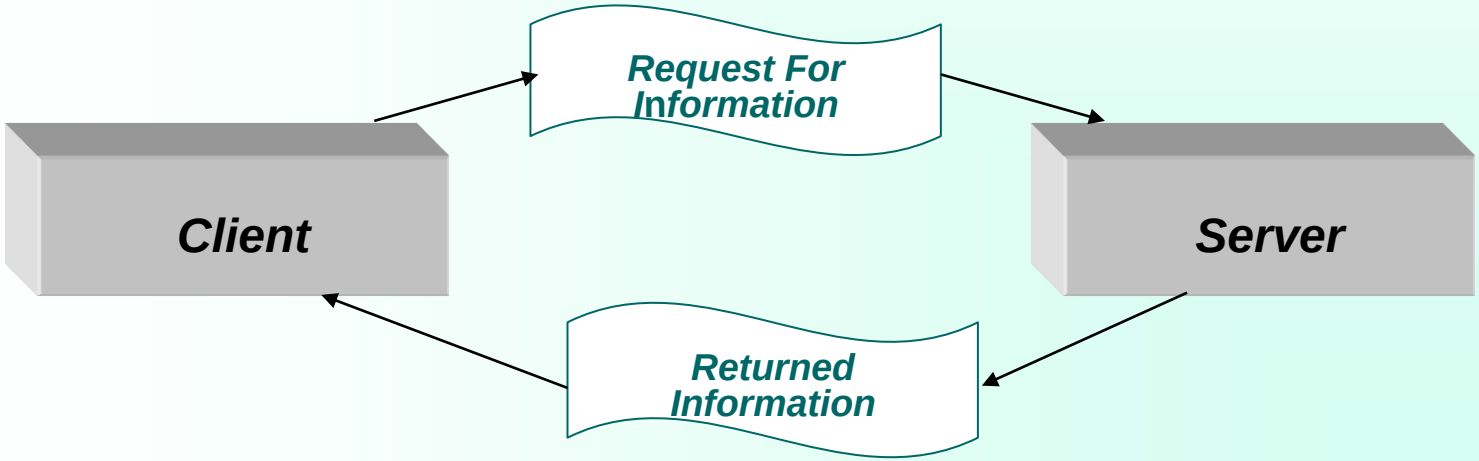
برنامه‌اي است كه روي ماشين سرويس‌دهنده نصب ميشود و منتظر است تا تقاضائي مبني بر برقراري يك ارتباط دريافت كرده و پس از پردازش آن تقاضا ، پاسخ مناسب را ارسال نمايد بنابراين در حالت كلي برنامه سرويس دهنده شروع كننده يك ارتباط نيست.

برنامه های سمت مشتری Client Side

برنامه هاي سمت مشتري بنابر نياز ، اقدام به درخواست اطلاعات مي‌نمايند.

تعداد مشتريها روي ماشينهاي متفاوت يا حتي روي يك ماشين مي‌تواند متعدد باشد

و ليكن معمولاً تعداد سرويس دهنده ها يكي است .(مگر در سيستم‌هاي توزيع‌شده)



ارتباط بين سرويس دهنده و مشتري

الگوریتم کار برنامه سمت سرویس‌دهنده

الف) Socket():

اعلام درخواست ارتباط و تعیین نوع آن (TCPیا UDP) از سیستم‌عامل با این تابع سیستمي

ب) Bind():

نسبت دادن يك آدرس پورت سوكتي كه باز كرده ايم

ج) Listen():

اعلام شروع پذيرش تقاضاهاي ارتباط TCP با اين تابع به سيستم عامل و تعين حداكثر تعداد پذيرش ارتباط TCP

د) Accept():

تقاضاي معرفي يكي از ارتباطات معلق با استفاده از اين تابع از سيستم عامل

ه) Send(),recv():

مبادله داده

و) Close():

قطع ارتباط دو طرفه ارسال و دريافت

ز) Shutdown(): قطع يك طرفه يكي از عمليات ارسال يا دريافت

الگوریتم کار برنامه سمت مشتری

الف) **Socket()**: ایجاد يك سوكت (مشخصه يك ارتباط)

ب) **Connect()**: تقاضاي برقراري ارتباط با سرويس‌دهنده

ج) **Send(),recv()**: ارسال و دريافت داده ها

د) **Close()**: قطع ارتباط بصورت دو طرفه .

Shutdown(): قطع ارتباط بصورت يك طرفه.

توابع مورد استفاده در برنامه سمت سرویس‌دهنده (مبتنی بر TCP)

- تابع socket()
- تابع Bind()
- تابع Listen()
- تابع Accept()
- توابع Send(),recv()
- توابع Close(),shutdown()

توابع مورد استفاده در برنامه مشتری (مبتنی بر پروتکل TCP)

- تابع socket()
- تابع Connect()
- توابع Send(),recv()
- توابع Close(),shutdown()

امکانات زبان جاوا

جاوا زباني است شيئ‌گرا ، ساده ، ايمن ، قابل حمل ، توانمند در حمايت از برنامه‌هاي چند ريسماني با معماري خنثي

تفاوت‌هاي زبان جاوا با زبانهاي C,C++:

- اشاره گرها
- استراکچرها و یونیون‌ها
- توابع
- وراثت چندگانه
- رشته‌ها
- goto
- Operator overloading
- تبديل خودکار نوع
- آرگومانهاي خط فرمان
- شيئ گرايي
- مفسر زمان اجراي جاوا

اپلت Applet

- ريزبرنامه يا برنامة كوچكي است كه درون يك صفحة وب قرار مي‌گيرد و روي يك سرويس‌دهندة اينترنت قابل دسترسي بوده و به عنوان بخشي از يك سند وب بر روي ماشين مشتري اجرا مي‌شود.

- برنامة اجرايي است و براي اجرا در محيط مرورگر در نظر گرفته شده تا قابليتهايي كه صفحات وب ندارند از طريق آنها فراهم شود.

- اپلت‌ها با برچسب APPLET درون صفحة وب تعريف مي‌شوند ولي فايلي خارجي به حساب مي‌آيند

دو راه اجرای یک اپلت

- اجرانمودن اپلت داخل يك مرورگر سازگار با جاوا مثل Netscape Navigator
- استفاده از Applet Viewer

محدوديتهای اپلت

- عدم دسترسي به سيستم فايل جز در موارد محدود
- عدم توانايي در فراخواني و اجراي برنامه در ماشين اجراكننده آن