
بسم الله الرحمن الرحيم

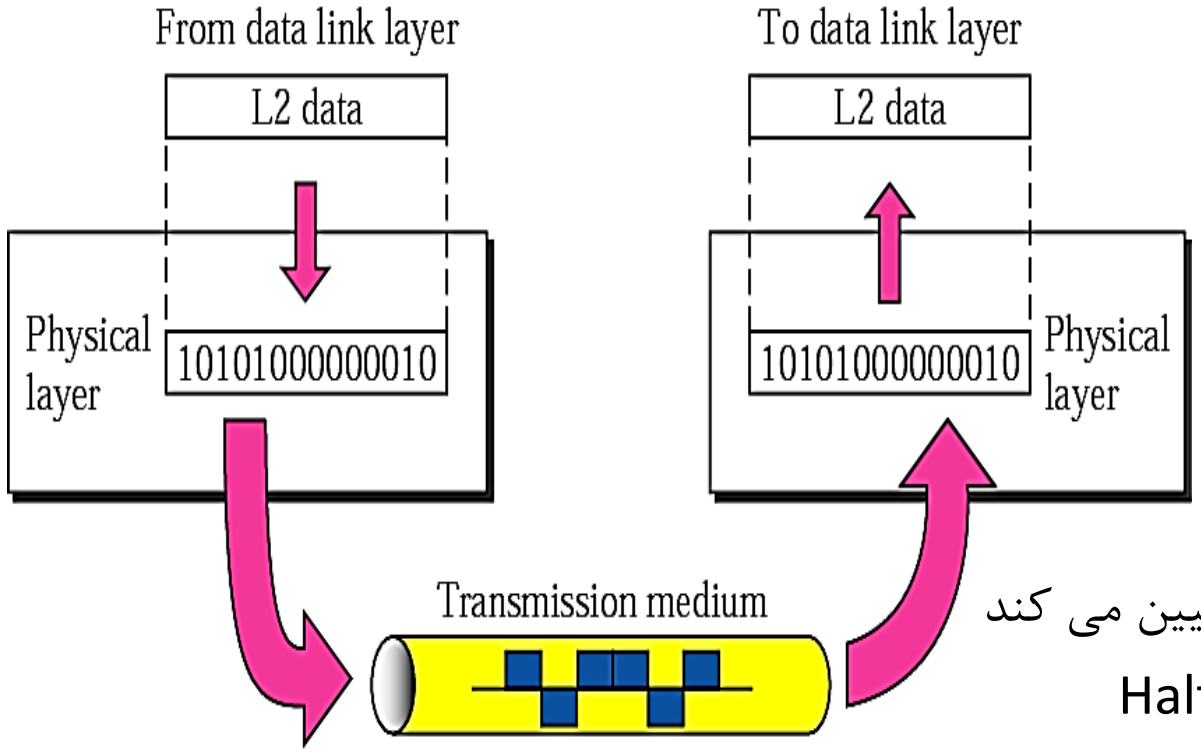
# لایه ها در مدل OSI

## لایه فیزیکی

وظیفه اصلی این لایه انتقال بیتها بر روی کانال مخابراتی است.در این لایه واحد اطلاعات بیت است و این واحد هیچ درکی از محتوی پیام ندارد. تنها چیزی که متوجه می شود بیتهای صفر و یک می باشد.

لایه فیزیکی مسئول جابجایی بیت ها از یک گره به گره بعدی است.

لایه فیزیکی به موارد دیگر هم رسیدگی می کند:




۱- تعیین نوع محیط فیزیکی و رابط بین وسایل و محیط انتقال.

۲- نمایش بیت ها: داده لایه فیزیکی دنباله ای از بیت ها است.

برای انتقال بیتها باید آنها را به صورت سیگنال الکتریکی یا نوری درآورد.چگونگی تبدیل صفرها و یک ها به سیگنال را سیگنال سازی یا Encoding می گویند.

۳- نرخ بیت: تعداد بیتی که در هر ثانیه ارسال می شود.

۴- حالت انتقال: لایه فیزیکی جهت انتقال اطلاعات بین دو وسیله را تعیین می کند که می تواند به صورت یک طرفهsimplex، نیمه دو طرفه Half duplex یا کاملا دو طرفه Full duplex باشد.

## پارامترهای مطرح درلایه فیزیکی

- ماهیت  فیزیکی خط انتقال
- چگونگی نمایش بیتها در قالب سیگنالی متناسب با کانال
- ظرفیت کانال فیزیکی و نرخ ارسال
- نوع ماژولاسیون
- چگونگی کوپلاژ فرستنده و گیرنده
- مسائل مکانیکی و الکتریکی

## لایه پیوند داده

وظیفه این لایه آن است که با استفاده از مکانیزمهای کشف و کنترل خطا داده ها را روی یک کانال انتقال که بدلیل وجود نویز ذاتا دارای خطاست بدون خطا و مطمئن به مقصد برساند.

ماهیت خطا به گونه ایست که قابل رفع نیست ولی می توان تدابیری وجود دارد که از سلامت داده ها اطلاع یابد و داده های خراب را دور بریزد

1. با استفاده از Parity
2. Checksum
3. CRC

رسیدن و یا نرسیدن اطلاعات نیز از زمره وظایف این لایه است

آدرس دهی فیزیکی، تعیین نحوه دسترسی به رسانه و مدیریت کانال وظیفه این لایه است. لایه فیزیکی به کمک این لایه به یک لینک ارتباطی قابل اطمینان تبدیل می شود.

سایر وظایف لایه پیوند داده:

1. کنترل جریان flow control
2. کنترل خطا error control
3. کنترل دسترسی: وقتی که دو یا چند وسیله به لینک مشترکی متصل می شوند باید مشخص شود در هر لحظه چه کسی می تواند از آن لینک استفاده کند.

PDU ارسالی از لایه پیوند داده ها در اصطلاح با اسم خاص "فریم" یا "قاب" گفته می شود.

از وظایف لایه پیوند داده مقابله با تصادم است از جمله قرارداد هایی که در این لایه قرار داده شده زیر لایه MAC است که در اصطلاح آن را لایه دو و نیم نیز می نامند.

راه اندازی سرویس گیری و کنترل سخت افزار در لایه فیزیکی بر عهده لایه پیوند داده است و در سطح سخت افزار صورت می گیرد.

## لایه شبکه

این لایه مسئول تحویل بسته های اطلاعات از ماشین مبدا در یک شبکه به ماشین مقصد در شبکه دیگر است.

آدرس دهی منطقی، کنترل ازدحام (congestion control)، مسیریابی بین کامپیوترهای فرستنده و گیرنده، تحویل داده به گیرنده به صورت نامطمئن از وظایف این لایه است.

مهمترین وظیفه این لایه مسیریابی است  هرگاه یک قطعه داده دارای هویت و شناسنامه تحویل این لایه شود ابتدا باید مشخص گردد که مقصد نهایی آن همین ماشین است و محتوی بسته باید تحویل لایه بالاتر گردد یا برای رسیدن به مقصد نهایی خود از طریق کانال دیگری به بیرون ارسال گردد.

در این لایه داده های دریافتی از لایه بالاتر باید در قالب بسته هایی با ساختار استاندارد سازماندهی شود (Packet) با توجه به آنکه مسیرهای گوناگونی وجود دارد. لذا این لایه وظیفه دارد هر بسته اطلاعاتی را پس از دریافت به مسیری هدایت کند تا آن بسته به مقصد برسد.

## لایه انتقال

این لایه مسئول تحویل پیغام از برنامه مبدا به برنامه مقصد است.

لایه شبکه یک بسته اطلاعاتی را به ماشین مقصد می رساند و لایه انتقال کل پیغام را به برنامه مقصد (در ماشین مقصد) می رساند.

ارائه سرویس برای تحویل داده به صورت مطمئن همراه با کشف خطای انتقال کنترل جریان داده، شکستن و قطعه قطعه کردن اطلاعات و شماره گذاری آنها برای این که قطعه ای گم نشود یا دوباره دریافت نشود از وظایف این لایه است.

لایه انتقال می تواند اتصال گرا (connection-oriented) یا فاقد اتصال (connectionless) باشد.

گرفتن داده از لایه های بالاتر و تقسیم آن به قطعات کوچکتر و ارسال آن به لایه شبکه و حصول اطمینان از دریافت صحیح آنها.

ایزوله کردن لایه های بالاتر در برابر تغییرات اجتناب ناپذیر سخت افزاری

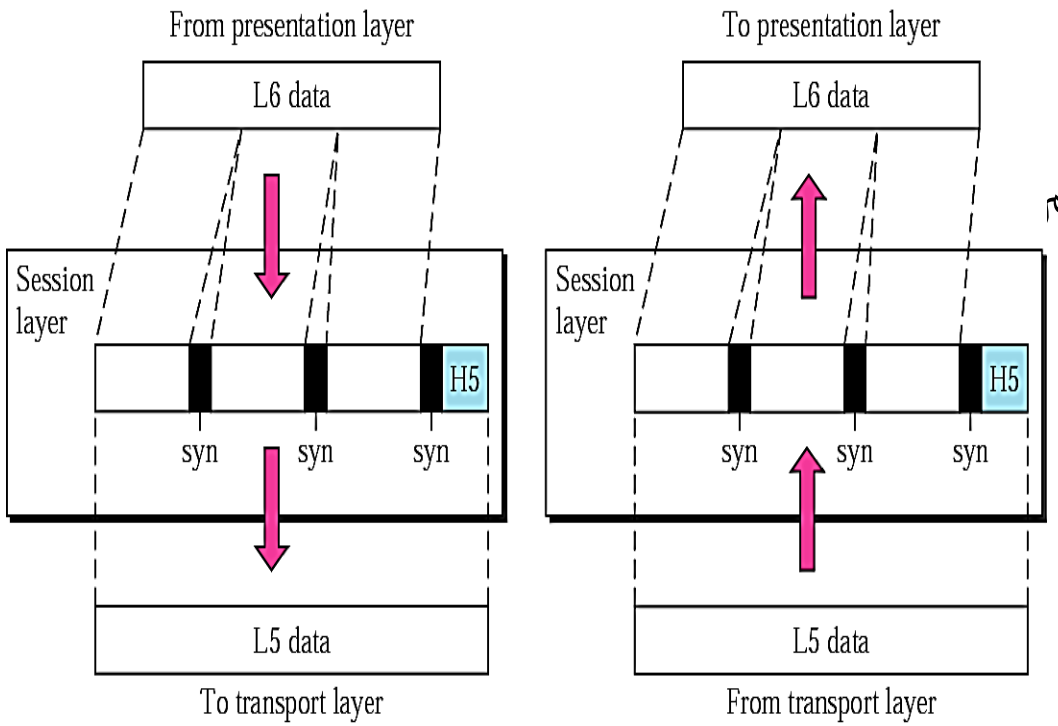
این لایه اولین لایه است که لایه های همتا با هم ارتباط نظیر به نظیر با یکدیگر برقرار می کنند.

## لایه جلسه کاری session

ایجاد، مدیریت و اتمام جلسه بین دو کامپیوتر، همزمان سازی تبادل داده بین فرستنده و گیرنده با قرار دادن نقاط وارسی از وظایف ایـن لایه است.

این لایه اجازه می دهد تا کاربران در ماشینهای مختلف نشست برقرار شود.

1. کنترل دیالوگ Dialog control اینکه نوبت چه کسی است
2. مدیریت نشانه token management جلوگیری از تداخل اعمال مهم
3. سنکرون کردن Synchronization کنترل عملیات انتقال طولانی مدت و از سرگیری از نقطه قطع شده



## لایه نمایش

تبدیل کدهای مختلف داده (ترجمه)

رمزگذاری داده در سمت فرستنده و رمزگشایی آن در سمت گیرنده

فشرده سازی داده و از حالت فشرده خارج کردن از وظایف این لایه است.

در این لایه تمرکز بر روی ساختار و مفهوم پیام است.

کامپیوترهایی که دارای ساختار متفاوت هستند برای آنکه بتوانند با یکدیگر ارتباط بر قرار کنند باید بر روی ساختار پیام به صورت مشخص و استاندارد توافق کنند که از وظایف لایه نمایش مدیریت این ساختارها در سطح بالاست

## لایه کاربرد

این لایه سرویس های شبکه ای لازم را برای برنامه های کاربردی و کاربران فراهم می کند.

برنامه های مرورگر وب، ایمیل، انتقال فایل و ... در این لایه قرار دارند.

با وجود مشخص شدن وظایف هر لایه مدل OSI یک معماری شبکه نیست زیرا پروتکل های آن پیاده سازی نشده اند. بسیاری از پروتکلهای مورد نیاز کاربران در لایه کاربرد قراردارد نظیر

HTTP

FTP

SMTP,POP3

NNTP

## پشته پروتکلی TCP/IP

پشته پروتکل TCP/IP قبل از مدل OSI ساخته شد به همین لایه های پشته پروتکل TCP/IP منطبق بـا لایـه هـای مـدل OSI نیستند.

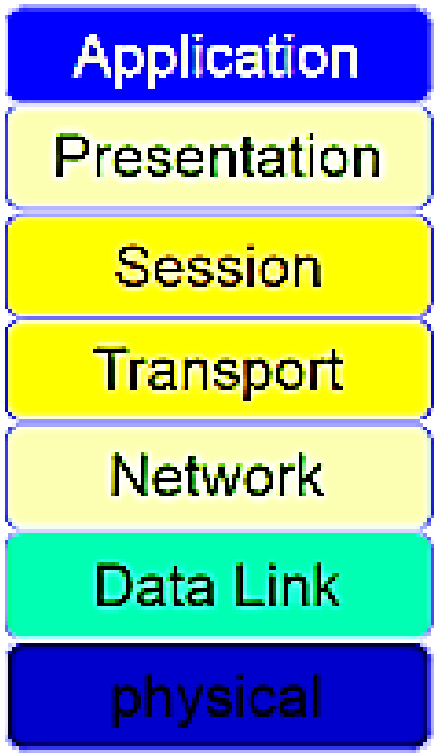
وزارت دفاع آمریکا این مدل را به عنوان مدل مرجع ایجاد کرد چون به شبکه ای نیاز داشت تا تحت هر شرایطی حتی جنـگ هسته ای پایدار بماند.

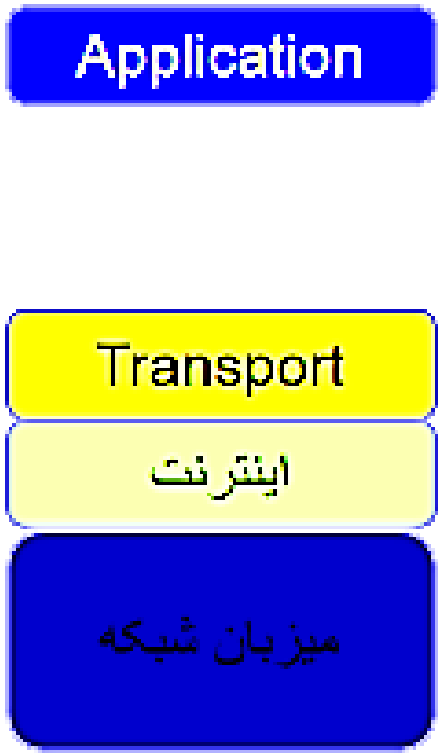
پشته پروتکل TCP/IP از ۴ لایه ساخته شده است: فیزیکی، پیوند داده، شبکه انتقال و کاربرد.

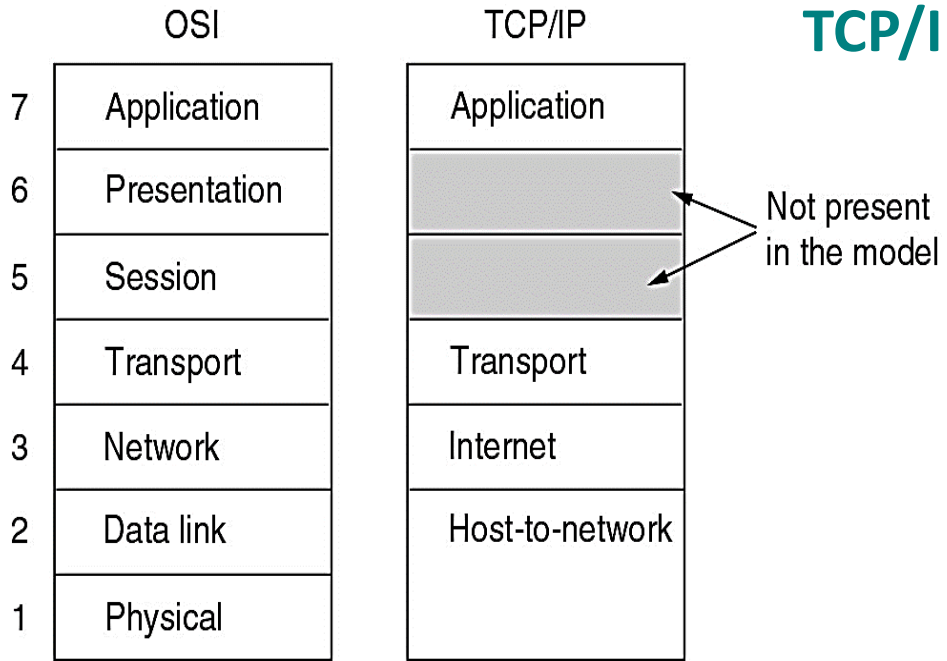
این پشته از ماجول هایی ساخته شده که هر کدام کار خاصی را انجام می دهد.

ماجول ها به هم وابسته نیستند اما با هم کار می کنند.

## مدل مرجع TCP/IP



لایه کاربرد: پیاده سازی پروسه های کاربردی در میزبانها.
لایه حمل: ارسال انتها به انتهای مطمئن بین پروسه های کاربردی.
لایه شبکه: آدرس دهی در سطح شبکه و مسیریابی.
لایه میزبان شبکه: آدرس دهی ترمینالها در سطح شبکه محلی و ساخت فریم های مناسب فضای انتقال فیزیکی و کنترل دسترسی به فضای انتقال.
لایه فیزیکی: سخت افزار و تجهیزات فیزیکی مخابرات داده.

## لایه اینترنت internet layer

در این لایه ، یک شبکه Packet switching مبتنی بر ارتباط غیر متصل انتخاب شده است و در واقع این لایه سنگ بنای معماری TCP/IP است .
وظیفه اصلی این لایه اینست که به ماشینها اجازه دهد بسته های خود را روی شبکه و به سمت مقصد بفرستد.
این لایه رسیدن بسته ها را به سمت مقصد تضمین نمی کند.
پیامها را مرتب نمی کند و این وظیفه به عهده لایه های بالاتر است.
فرمت بسته ها در این لایه به صورت IP تعریف می شود.(Internet Protocol)

## لایه انتقال

وظایف این لایه مشابه وظایف لایه انتقال مدل OSI است .
انتقال به صورت نقطه به نقطه صورت می گیرد.
دو پروتکل اصلی در این مدل وجود دارد

1. TCP (Transmission Control Protocol)
2. UDP (User Datagram Protocol)

## وظایف مشترک بین لایه های مدل مرجع اینترنت

_مالتی پلکس کردن

_کنترل خطا

_کنترل استفاده از منابع

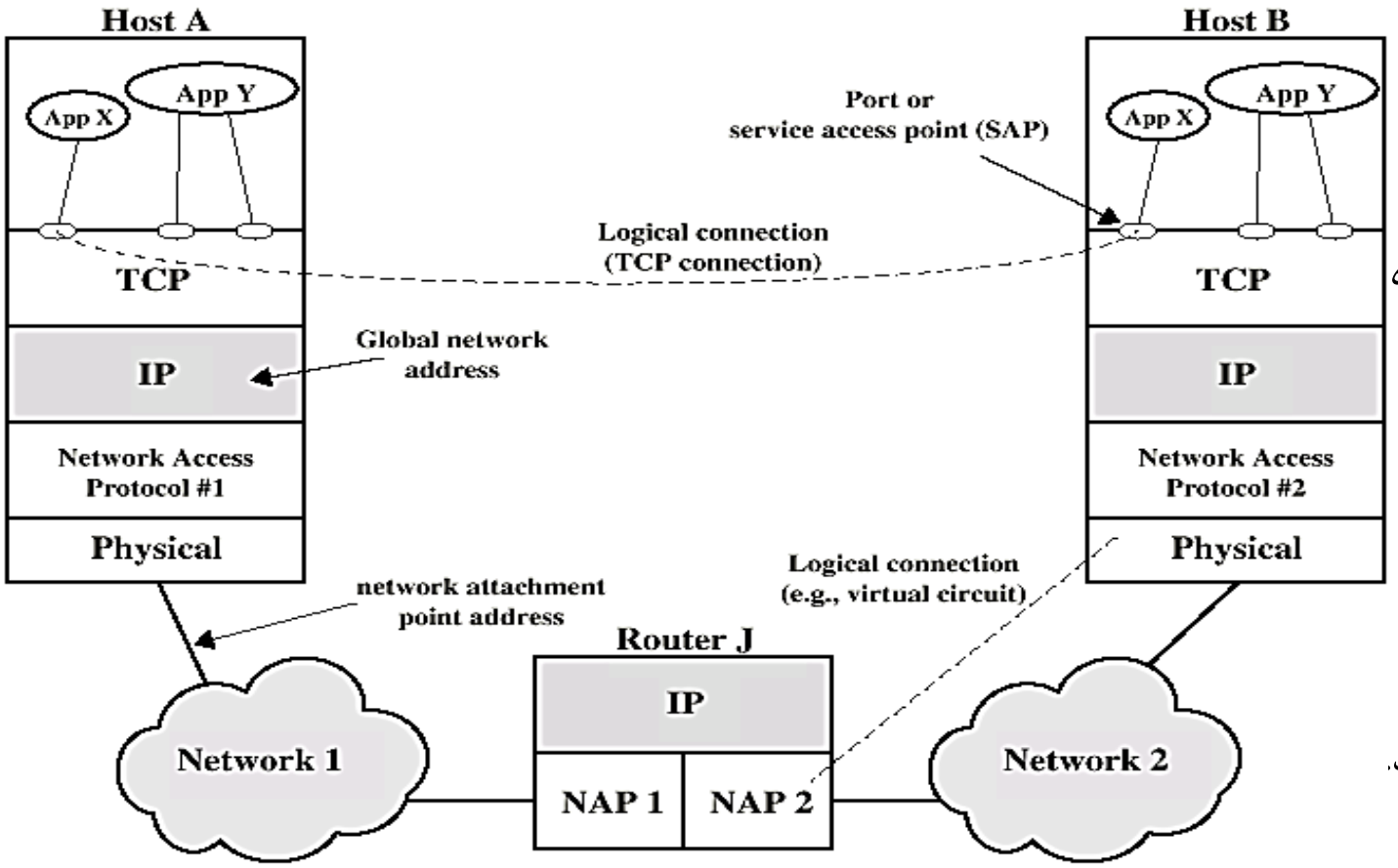
_ همگام سازی بین فرستنده و گیرنده و کنترل جریان ارسال داده

_آدرس دهی و نامگذاری به منظور شناسایی پروسه های متناظر

+در سطح لایه ۲ بصورت گره به گره

+در سطح لایه ۳ بصورت ترمینال به ترمینال

+در سطح لایه ۴ و ۵ بصورت نرم افزار به نرم افزار




## تفاوت ها و شباهت های ما بین OSI و TCP/IP

✓ هر دو مدل به صورت لایه ای طراحی شده اند.

✓ هر دو لایه دارای لایه های انتقال و شبکه شبیه یکدیگر هستند.

✓ هر دو از تکنولوژی سوییچ بسته استفاده می کنند.

✓ تفاوت های دو مدل:

✓ مدل TCP/IP لایه ارائه و جلسه OSI را در لایه کاربردی ادغام کرده است.

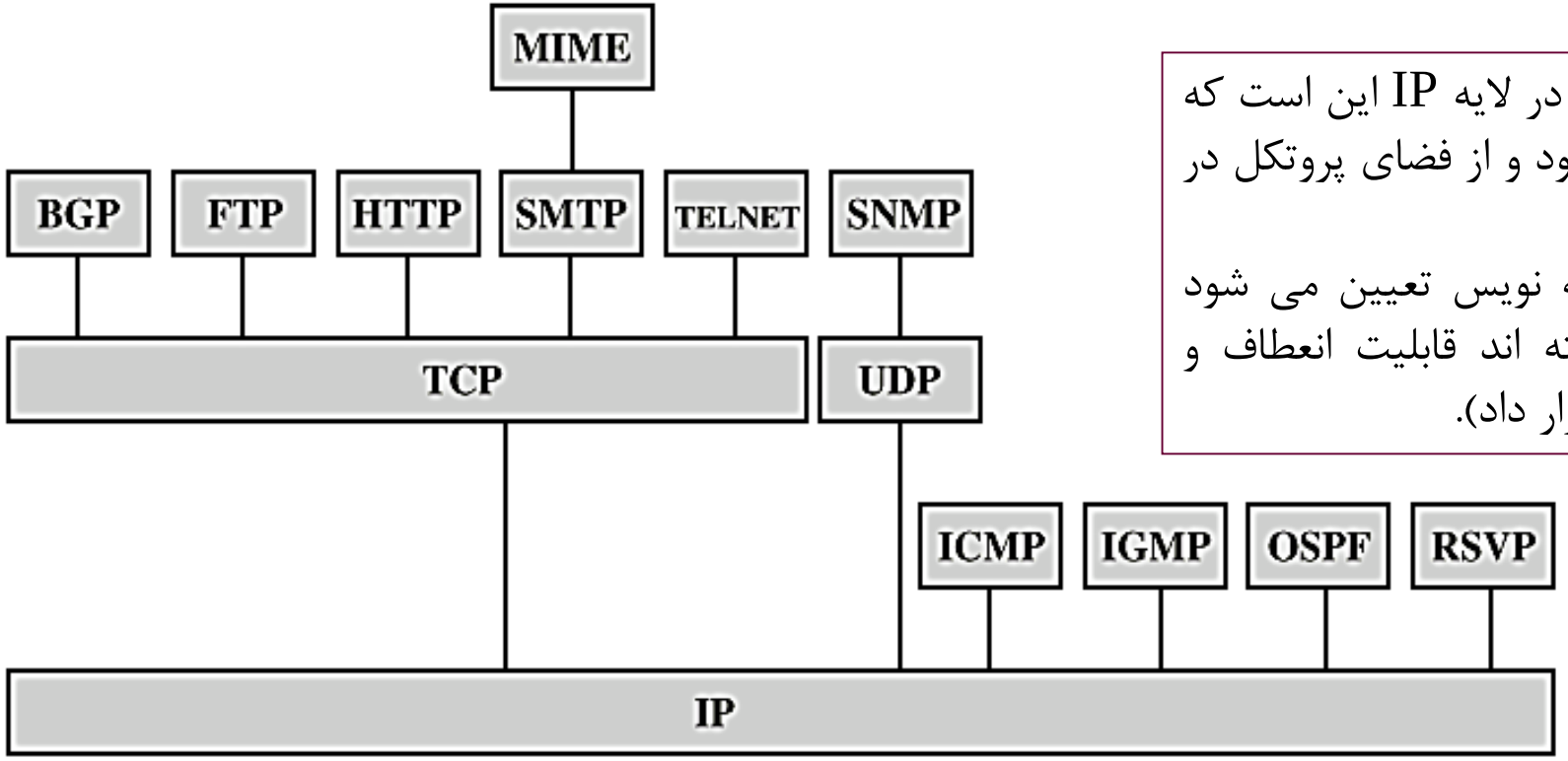
✓ مدل TCP/IP لایه پیوند داده و فیزیکی را در یک لایه قرار داده است.

✓ TCP/IP به علت تعداد لایه های کمتر ساده تر به نظر می رسد.

✓ پروتکل TCP/IP استاندارد اینترنت است در حالی که اکنون از پروتکل های SNA (پیاده سازی OSI) استفاده نمی شود.

# پروتکلها در اینترنت

در شکل زیر تعدادی از پروتکلهای مورد استفاده در لایه های مختلف در اینترنت نشان داده شده اند:




علت قرار گرفتن ICMP,IGMP,OSPF,RSVP در لایه IP این است که برای این پروتکل ها port number تعریف نمی شود و از فضای پروتکل در هدر IP استفاده می کنند .
با توجه به اینکه port number ها توسط برنامه نویس تعیین می شود سایر پروتکل های کاربردی در TCP قرار گرفته اند قابلیت انعطاف و گسترش مناسبی دارند. ( اینها را نمی توان در IP قرار داد).

از پروتکلهای مورداستفاده در شبکه های کامپیوتری می توان به TCP, IP, UDP, HTTP, FTP, BGP و RSVP اشاره کرد.

BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = Hypertext Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
MIME = Multi-Purpose Internet Mail Extension
OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

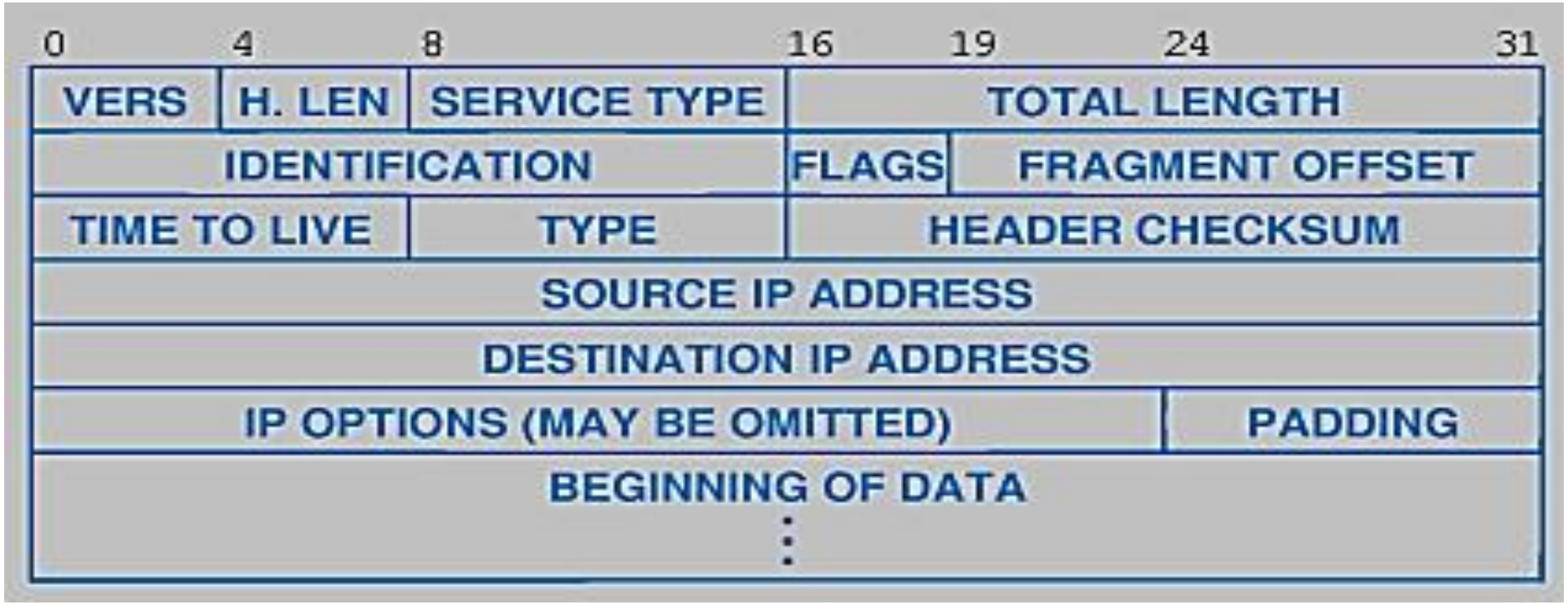
# پروتکل IP

Internet Protocol_

_مدل Best Effort بر مبنای روش دیتاگرام برای ارسال بسته ها از مبدا به مقصد

_مسیریابی بر اساس آدرسهای ۳۲بیتی IP

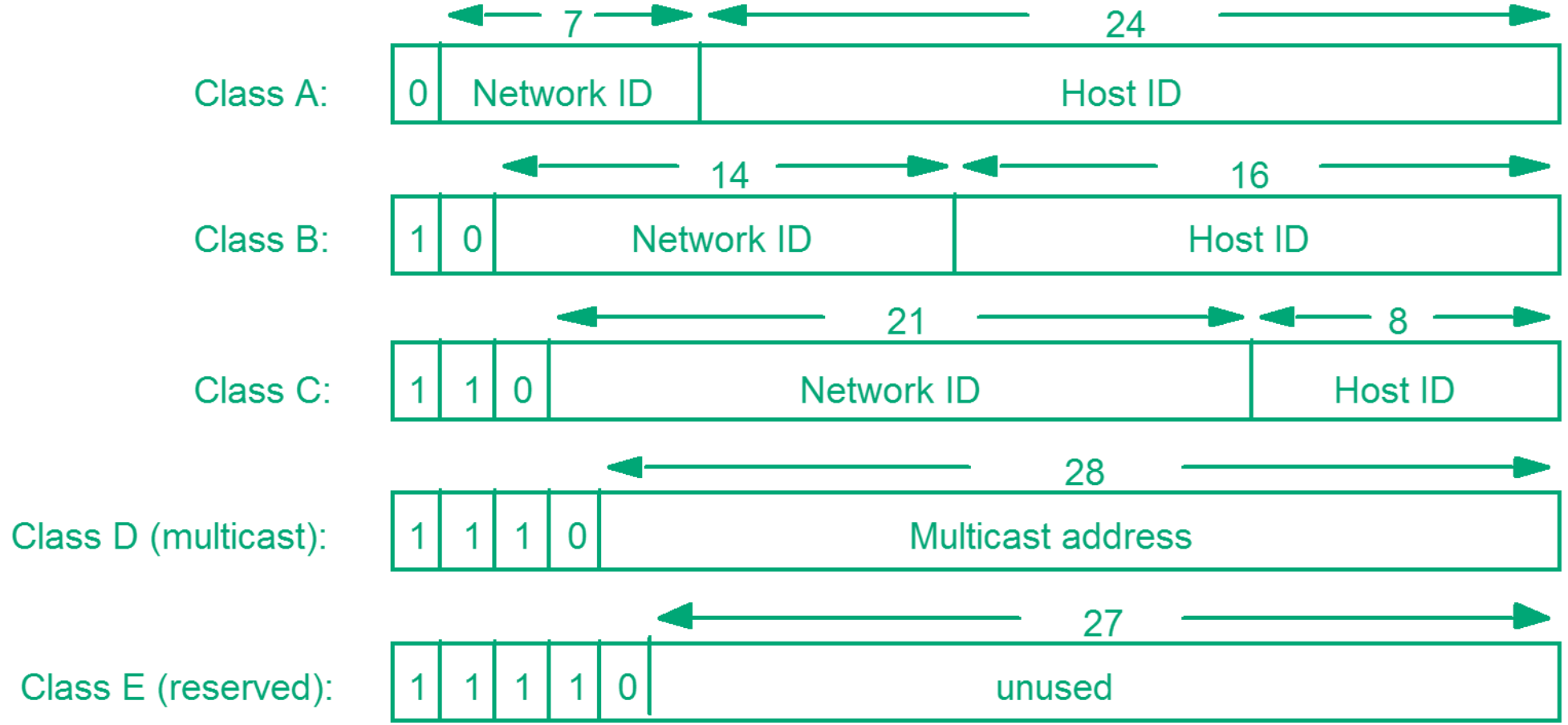
_فرمت بسته های IP بشکل زیر است:




- IP بیست بایت سرآمد ثابت به اضافه یک بخش با طول متغیر به بسته اضافه می کند.

# آدرس دهی در اینترنت

چهار نوع آدرس D،C،B،A در اینترنت استفاده می شود که با پیشوندهای مختلف از هم مشخص می شوند:

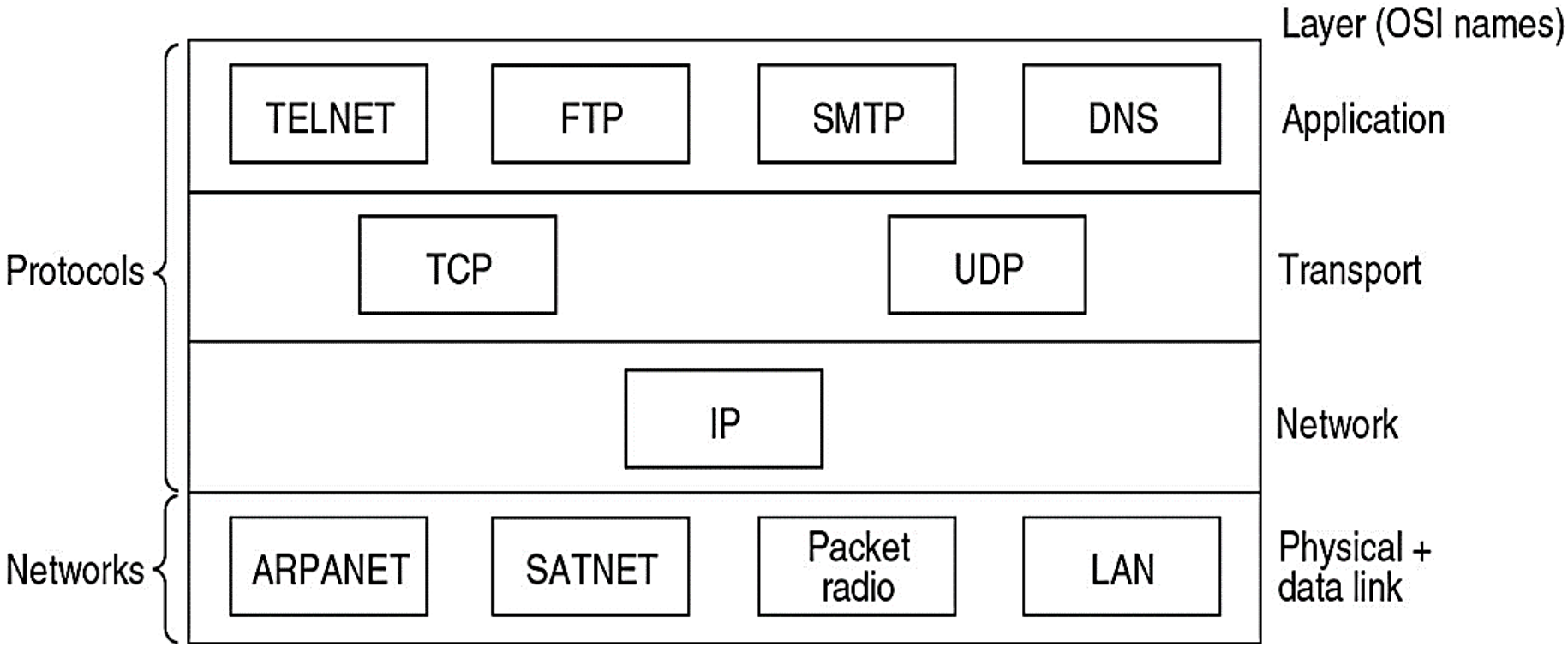



در حال حاضر برای آنکه فضای آدرس بصورت قابل انعطاف و با راندمان بیشتری استفاده شود, نوع classless استفاده می شود. در این نوع, بخش network ID در آدرس از این قواعد پیروی نمی کند و می تواند هر طول دلخواهی داشته باشد (مقدار حداقل آن ۲ بیت و مقدار حداکثر آن به طول بخش host ID بستگی دارد).

# پروتکل TCP

یک پروتکل اتصال گرا است قابل اعتماد است (Connection Oriented Best Effort) است. پروتکل IP یک سرویس connectionless غیر قابل اتکا ارائه می کند. پروتکل TCP برروی IP قرار گرفته و با اجرای الگوریتم پنجره لغزان یک سرویس connection-oriented قابل اتکا reliable به لایه بالای خود ارائه می کند.

اجازه می دهد تا جریانی از بایتها بدون خطا از یک کامپیوتر به کامپیوتر دیگر فرستاده شود. جریان بایت را به صورت بسته در آورده و به لایه اینترنت تحویل داده می شود. در ماشین مقصد این پروتکل بسته ها را به یکدیگر الحاق کرده تا جریانی از بیتها را بدست آورد. کنترل جریان داده نیز در این لایه صورت می گیرد و فرستنده سریع سرعت خود را با گیرنده کند هماهنگ می کند.



# سیستم عامل شبکه

# مراحل راه اندازی یک شبکه

برای راه اندازی هر نوع شبکه ای مراحل زیر را باید طی کرد.

۱. طراحی (Design)

۲. تنظیمات (Roll Out)

۳. پیکربندی (Configuration)

۴. مدیریت (Management)

### ۱- طراحی شبکه (Design)

فاز طراحی معمولاً یک الی سه روز طول میکشد که بستگی به بزرگی شبکه و کار آن دارد.

نکاتی که در فاز طراحی باید به آنها توجه کرد:

۱. شبکه Peer-to-Peer است یا Client/Server

۲. انتخاب نرم افزار شبکه

۳. انتخاب زبان شبکه

۴. تهیه لیست سخت افزارهای موردنیاز

۵. تعیین میزان سطح امنیت اطلاعات

۶. یادگیری راه  حل های نرم  افزاری و سخت  افزاری برای رفع مشکلات مدیریتی روزمره

### ۲- تنظیمات شبکه (Roll Out)

برای تنظیم کردن شبکه مراحل زیر را باید انجام داد:

۱. آزمایش کابل ها

۲. نصب یک یا چند سِرور، اگر شبکه از نوع مدل Client/Server باشد.

۳. نصب سخت  افزار کامپیوتر های دیگر (گروه کاری)

۴. اتصال کارت های شبکه به کابل ها (NIC-کارت شبکه باعث اتصال کامپیوتر ها به شبکه می شود.)

۵. نصب یک یا چند Hub (اگر از کابل Twisted Pair استفاده می شود. در این نوع شبکه  ها از توپولوژی Star استفاده مـی شود. )

۶. نصب چاپگر ها

۷. نصب برنامه سرویس دهنده (سیستم عامل شبکه یا NOS) اگر مدل شبکه Client/Server است

۸. نصب برنامه روی کامپیوتر های دیگر

۹. نصب برنامه  های کاربردی

### ۳- پیکربندی شبکه (Configuration)

پیکربندی شبکه به معنای سفارشی کردن آن برای کاربر است.

۱. ایجاد حساب های دسترسی به شبکه برای کاربران (نام کاربری- کلمه عبور- گروه کاری)
۲. تخصیص فضایی از هارد دیسک برای به اشتراک گذاشتن فایلها و داده های کاربران
۳. تخصیص فضایی از هارد دیسک برای به اشتراک گذاشتن برنامه ها توسط کاربران
۴. تنظیم نوبت چاپ (نرم افزاری که اجازه میدهد کاربران از چاپگر های شبکه استفاده کنند)
۵. نصب سیستم پشتیبانی شبکه برروی ایستگاه های کاری کاربران

### ۴- مدیریت و اداره شبکه (Management)

۱. نقشه برداری از شبکه به منظور مدیریت و اشکال زدایی آسانتر
۲. نصب سطوح امنیتی مناسب به منظور جلوگیری از خسارات عمدی و سهوی
۳. بالا بردن سرعت شبکه از طریق تنظیم LAN
۴. ایجاد استانداردهای شرکت برای اضافه کردن سخت افزار و نرم افزار. با این کار میتوان از بروز مشکلات در آینده جلوگیری کرد.

## آشنایی با آدرس‌های IPv4

آشنایی با آدرس‌های IP یکی از نکات کلیدی در درک نحوه عملکرد پروتکل IP می‌باشد. آدرس IP یک شناسه عددی است که به هر دستگاه در شبکه‌های IP اختصاص داده می‌شود. این نوع از آدرس‌ها، در واقع آدرس‌های منطقی هستند که برای تشخیص محل قرارگیری دستگاه‌ها به کار برده می‌شوند و با آدرس‌های فیزیکی (MAC Address) که به کارت واسط شبکه (NIC) اختصاص داده می‌شوند متفاوت هستند.

در این فصل، فرض بر این است که شما با نشانه‌گذاری اعداد در مبنای ۲ و نحوه تبدیل مبناها آشنا هستید. بنابراین تا حد امکان از ذکر جزئیات مربوط به تبدیل مبناها خودداری شده است.

## معرفی آدرس IPv4

یک آدرس IPv4 از ۳۲ بیت (۰ یا ۱) تشکیل شده است. این بیت‌ها به چهار قسمت ( که Octet یا Quad نامیده می‌شود) تقسیم شده‌اند و هر قسمت حاوی یک بایت (۸ بیت) می‌باشد. سه روش رایج جهت نمایش یک آدرس IP وجود دارد:

- دهدهی[1] (مبنای ده)، مانند 130.57.30.56
- دودویی[2] (مبنای دو)، مانند 10000010.00111001.00011110.00111000
- شانزده‌دهی[3] (مبنای شانزده)، مانند 82 39 1E 38

همه مقادیری که در بالا مشاهده می‌نمایید، بیانگر آدرس IP یکسانی می‌باشند. با ۳۲ بیت موجود در آدرس‌های IPv4، مجموعاً تعداد ٤،٢٩٤،٩٦٧،٢٩٤ = $2^{32}$ آدرس از این نوع قابل ایجاد می‌باشد.

---

1. Decimal
2. Binary
3. Hexadecimal

## ساختار آدرس IP

بطور کلی آدرس‌های IP از دو شناسه تشکیل شده‌اند. یکی شناسه شبکه (NetworkID) و دیگری شناسه میزبان (HostID). هر کدام از این شناسه‌ها بسته به نوع کلاس آدرس IP تعیین می‌شوند.

### شناسه شبکه

این شناسه، آدرس یک زیرشبکه را تعیین نموده و برای کلیه میزبان‌هایی که در یک زیرشبکه قرار دارند یکسان می‌باشد. شناسه شبکه در واقع یک ساختار سلسله مراتبی یا لایه‌ای به آدرس‌های شبکه می‌دهد. به عنوان مثال آدرس 130.57.30.56 را در نظر بگیرید. این آدرس از کلاس B بوده و دو قسمت اول آن به عنوان شناسه شبکه در نظر گرفته می‌شود، بنابراین کلیه کاربرانی که در زیرشبکه‌ای با این آدرس قرار داشته باشند دو قسمت اول آدرس IP آنها با 130.57 شروع می‌شود.

### شناسه میزبان

آدرس یک دستگاه یا میزبان در شبکه است و برای هر میزبان عددی منحصر بفرد می‌باشد. در مثال قبل، دو قسمت دوم از آدرس متعلق به شناسه میزبان می‌باشد، بنابراین در آدرس‌هایی مانند 130.57.30.56، آدرس 30.56. بیانگر شناسه میزبان زیرشبکه‌ای با آدرس 130.57 می‌باشد.

## کلاس‌های آدرس IP

بطور کلی سه کلاس آدرس‌دهی قابل اختصاص به کاربران توسط طراحان اینترنت به کار گرفته شده است. این کلاس‌ها با نام‌های A، B و C شناخته می‌شوند. برای شبکه‌های خیلی بزرگ که متشکل از چندین زیرشبکه می‌باشند از کلاس A، و برای شبکه‌های بسیار کوچک از کلاس C استفاده می‌شود. شبکه‌های متوسط نیز از کلاس B جهت آدرس‌دهی به کاربران خود استفاده می‌نمایند.

تقسیم‌بندی آدرس‌های IP به آدرس‌های شبکه و آدرس‌های میزبان (NetID و HostID) نیز بر اساس همین کلاس‌بندی‌ها انجام می‌شود. در جدول ۱-۱ خلاصه‌ای از مشخصات این سه کلاس آورده شده است.

جدول ۱-۱ : خلاصه‌ای از مشخصات کلاس‌های A، B و C

| کلاس | بیت‌های قاب زیرشبکه | الگوی بیتی راهنما | مقدار اولین اُکتت[1] در آدرس | تعداد شبکه‌های قابل اختصاص | حداکثر میزبان‌ها در هر شبکه |
|---|---|---|---|---|---|
| A | 8 | 0 | 1-126 | 126 | 16,777,214 |
| B | 16 | 01 | 128-191 | 16,384 | 65,534 |
| C | 24 | 110 | 192-223 | 2,097,152 | 254 |

1. Octet

همانطور که در جدول مشاهده می‌کنید، ستونی جهت نشان دادن الگوی بیت‌های راهنما برای هر کلاس در نظر گرفته شده است. این بیت‌ها در واقع بیت‌های شروع آدرس‌های هر کلاس را نشان می‌دهند. به عنوان مثال، آدرس 126.x x x را در کلاس A درنظر بگیرید. قسمت اول این آدرس عدد 126 است که معادل دودویی آن 01111110 می‌باشد، بنابراین در ستون مربوطه، الگوی شروع این آدرس‌ها با 0 نشان داده شده است. در کلاس‌های B و C نیز اکتت اول کلیه آدرس‌ها به ترتیب با الگوی 01 و 110 آغاز می‌شوند و با تغییر آدرس‌ها در هر کلاس، به غیر از بیت‌های ذکرشده، سایر بیت‌ها تغییر می‌کنند. استفاده از این الگوهای بیتی در مسیریاب‌ها بسیار پرکاربرد می‌باشد زیرا این دستگاه‌ها می‌توانند با خواندن قسمت اول این آدرس‌ها الگوی بیتی آنها را بدون نیاز به دانستن سایر بیت‌ها تشخیص داده و از کلاس آن آدرس و همچنین قاب زیرشبکه[1] آن آگاهی یابند.

بعضی از آدرس‌های IP برای کاربردهای خاصی در نظر گرفته شده‌اند و قابل اختصاص به کاربران شبکه نمی‌باشند (البته به غیر از آدرس‌های خصوصی). در جدول ۱-۲ این آدرس‌ها به همراه کاربر آنها آورده شده است.

## آدرس‌های IP با کاربردهای خاص

| آدرس | کاربرد |
| --- | --- |
| آدرس 0.0.0.0 | بسته به قاب زیرشبکه، بیانگر همین شبکه (شبکه یا زیرشبکه‌ای که درحال حاضر در آن قرار دارید) یا همین میزبان می‌باشد. |
| آدرس‌هایی که با 127 شروع می‌شوند | این آدرس‌ها برای تست‌های loopback استفاده می‌شوند و به یک میزبان اجازه می‌دهند تا پیغام‌های تست را بدون اینکه ترافیکی در شبکه ایجاد کند، برای خود ارسال نماید. |
| آدرس 255.255.255.255 | این آدرس برای ارسال پیغام‌ها به تمام کاربران شبکه (Multicasting) استفاده می‌شود و با نام‌های limited broadcast و all-1s broadcast نیز شناخته می‌شود. |
| آدرس‌های<br>10.0.0.0 تا 10.255.255.255<br>172.16.0.0 تا 172.31.255.255،<br>192 168.0.0 تا 192.168.255.255 | این آدرس‌ها به عنوان **آدرس‌های خصوصی/نامعتبر**[2] برای کلاس‌های A، B و C در نظر گرفته شده‌اند. آدرس‌های خصوصی در استاندارد RFC 1918 تعریف شده و قابل استفاده در اینترنت نمی‌باشند. از این آدرس‌ها در سرورهای NAT و شبکه‌های IP غیرمتصل به اینترنت (شبکه‌های داخلی یا همان شبکه‌های خصوصی) استفاده می‌شود. |

1. Subnet mask
2. Private/Invalid

## کلاس A

در کلاس A بایت اول (۸ بیت اول از سمت چپ) برای آدرس شبکه و سه بایت باقیمانده برای آدرس میزبان استفاده می‌شود و فرمت آدرس‌های این کلاس به صورت Network.Host.Host.Host می‌باشد. به عنوان مثال در آدرس 49.22.102.70 عدد 49 آدرس شبکه و 22.102.70 آدرس میزبان را نشان می‌دهند. در این مثال، هر دستگاه در شبکه دارای یک آدرس متمایز به همراه آدرس شبکه 49 می‌باشد.

در کلاس A می‌توان از ۱۲۶ زیرشبکه استفاده نمود. علت این است که آدرس شبکه در این کلاس یک بایت است و اولین بیت از آن (با صفر) رزرو شده است، بنابراین هفت بیت باقیمانده در این بایت قابل استفاده می‌باشند. این بدین معناست که بیت‌های تشکیل دهنده این کلاس حداکثر می‌توانند دارای مقدار ۱۲۸ باشند (هر کدام از این هفت بیت می‌توانند مقدار ۰ یا ۱ را اختیار کنند که در مجموع $۲^۷$ یا ۱۲۸ موقعیت را فراهم می‌نمایند)، البته آدرس‌هایی که با 00000000 (بایت اول با بیت‌های صفر) و 01111111 (معادل با ۱۲۷ که آدرس‌های Loopback می‌باشند) شروع می‌شوند، رزرو شده هستند. بنابراین از ۱۲۸ موقعیت، دو موقعیت رزرو شده و در نهایت ۱۲۶ = ۲ – ۱۲۸ موقعیت در دسترس است، پس تعداد زیرشبکه‌های قابل آدرس‌دهی در کلاس A برابر با ۱۲۶ می‌باشند.

در این کلاس سه بایت آخر آدرس (۲۴ بیت آخر) متعلق به آدرس میزبان می‌باشد، به این معنا که ۱۶،۷۷۷،۲۱۶ = $۲^{۲۴}$ ترکیب متمایز از این ۲۴ بیت وجود دارد. چون آدرس‌های 0.0.0. و 255.255.255. رزرو شده هستند در نهایت تعداد ۱۶،۷۷۷،۲۱۴ = ۲ – $۲^{۲۴}$ آدرس قابل اختصاص به میزبان‌ها در کلاس A موجود می‌باشد.

**کلاس B**

در کلاس B، دو بایت اول به عنوان آدرس شبکه و دو بایت باقیمانده به عنوان آدرس میزبان در نظر گرفته می‌شوند. فرمت آدرس‌های این کلاس به صورت Network.Network.Host.Host می‌باشد. به عنوان مثال در آدرس 130.57.30.56، آدرس شبکه برابر با 130.57 و آدرس میزبان نیز 30.56 می‌باشد.

---

1. Automatic Private IP Addressing

تعداد بیت‌های آدرس شبکه در کلاس A برابر ۱۶ بیت می‌باشد، بنابراین تعداد $۲^{۱۶} = ۶۵،۵۳۶$ ترکیب متمایز از بیت‌ها وجود دارد. اما با توجه به نظر طراحان اینترنت مبنی بر اینکه آدرس‌های این کلاس باید با بیت‌های 01 شروع شوند، در نهایت ۱۴ بیت قابل استفاده است. بنابراین تعداد زیرشبکه‌ها در این کلاس برابر با $۲^{۱۴} = ۱۶،۳۸۴$ می‌باشد.

در کلاس B دو بایت آخر به عنوان آدرس میزبان در نظر گرفته می‌شود، این دو بایت نیز از ۱۶ بیت تشکیل شده‌اند، بنابراین $۲^{۱۶} = ۶۵،۵۳۶$ ترکیب متمایز برای آنها وجود دارد. چون آدرس‌های 0.0. و 255.255. (آدرس‌هایی که دو قسمت آخر آنها به شکل مذکور می‌باشد) رزرو شده هستند، تعداد میزبان‌های قابل آدرس‌دهی در این کلاس برابر با $۲^{۱۶} - ۲ = ۵۲۴،۶۵$ خواهد بود.

## کلاس C

در کلاس C سه بایت اول به عنوان آدرس شبکه و یک بایت باقیمانده به عنوان آدرس میزبان درنظر گرفته می‌شود. فرمت آدرس‌ها در این کلاس به صورت Network.Network.Network.Host می‌باشد. به عنوان مثال در آدرس 198.21.74.102، آدرس شبکه 198.21.74 و آدرس میزبان 102 می‌باشد.

آدرس‌های کلاس C با سه بیت 110 آغاز می‌شوند، بنابراین از ۲۴ بیتی که تشکیل‌دهنده آدرس شبکه در این کلاس هستند، ۳ بیت کسر شده و در نهایت تعداد ۲۱ بیت (قابل دستکاری) باقی می‌ماند. پس تعداد $۲^{۲۱}$ = ۲،۰۹۷،۱۵۲ زیرشبکه در کلاس C قابل ایجاد می‌باشد. الگوی بیتی 110 نشان دهنده عدد ۱۹۲ (11000000) بوده و با دستکاری سایر بیت‌ها تا عدد ۲۲۳ (11011101) نیز قابل مقداردهی می‌باشد، بنابراین روشی ساده برای تشخیص آدرس‌های کلاس C این است که اکتت اول با اعداد بین ۱۹۲ تا ۲۲۳ شروع شده باشد صرفنظر از اینکه اکتت‌های دوم و سوم دارای چه مقادیری باشند.

در کلاس C بایت آخر به عنوان آدرس میزبان درنظر گرفته می‌شود. پس با داشتن ۸ بیت تعداد ۲۵٦ = $۲^۸$ آدرس متمایز وجود خواهد داشت. چون دو آدرس 0. و 255. رزرو شده هستند در نهایت تعداد ۲۵٤ آدرس قابل اختصاص به میزبان‌ها در کلاس C قابل دسترسی می‌باشد.

دو کلاس دیگر از آدرس‌های IP، کلاس‌های D و E هستند. آدرس‌های کلاس D به آدرس‌های Multicast یا چندپخشی معروف هستند و برای موارد Multicasting یا ارسال پیغام‌ها به صورت همزمان به بیش از یک کاربر (چندپخشی) در شبکه استفاده می‌شوند. دامنه این آدرس‌ها از 224.0.0.0 تا 239.255.255.255 می‌باشد.

آدرس‌های کلاس E نیز جهت استفاده در آینده رزرو شده‌اند و دامنه آنها از 240.0.0.0 تا 255.255.255.255 می‌باشد. آدرس‌های این کلاس جهت موارد آزمایشی مورد استفاده قرار می‌گیرد.

## انجام سابنتیگ[1] در شبکه

زمانی که در یک سازمان بزرگ با تعداد زیادی از کامپیوترها سروکار دارید و یا این کامپیوترها از لحاظ جغرافیایی جدا از یکدیگر قرار دارند، می‌توان شبکه را به چندین شبکه کوچکتر تقسیم کرده و آنها را از طریق مسیریاب‌ها به یکدیگر متصل نمود. به هر کدام از این شبکه‌های کوچکتر یک زیرشبکه[2] گفته می‌شود. استفاده از زیرشبکه‌ها دارای مزایایی است که در ادامه آنها را بر می‌شماریم:

- کاهش ترافیک شبکه: زمانی‌که تعداد کامپیوترها در شبکه زیاد است، ارسال بسته‌ها به داخل شبکه می‌تواند موجب ایجاد ترافیک و در نتیجه مسدود شدن شبکه گردد. با استفاده از زیرشبکه و مسیریاب‌ها، بیشتر ترافیک در داخل هر زیرشبکه باقی مانده و بسته‌ها از طریق مسیریاب به سایر زیرشبکه‌ها ارسال می‌شوند. بنابراین با کاهش ترافیک، کارایی شبکه افزایش می‌یابد.
- مدیریت آسان: زمانی که بجای یک شبکه بسیار بزرگ، با تعدادی زیرشبکه کوچکتر مواجه باشید، مدیریت هر یک از این زیرشبکه‌های کوچک، بسیار ساده‌تر از مدیریت کل شبکه خواهد بود.

کلیه زیرشبکه‌ها در یک سازمان، دارای آدرس شبکه مشترکی می‌باشند که جهت شناسایی شبکه در این سازمان به کار می‌رود. اما علاوه بر آدرس شبکه، هر زیرشبکه باید دارای شماره‌ای باشد که بتوان آنرا از سایر زیرشبکه‌ها تشخیص داد. این شماره، آدرس زیرشبکه نامیده می‌شود.

استفاده از ساب‌نتینگ و زیرشبکه‌ها، چندین مشکل را در انجام آدرس‌دهی به میزبان‌ها برطرف می‌کند:

- اگر یک سازمان فقط دارای یک آدرس IP باشد ولی به چندین زیرشبکه فیزیکی نیاز داشته باشد، می‌توان با استفاده از ساب‌نتینگ و تقسیم این آدرس به چندین زیرشبکه، مشکل آدرس‌دهی در این سازمان را برطرف نمود.
- چون ساب‌نتینگ اجازه می‌دهد که تعداد زیادی از شبکه‌ها با یکدیگر تشکیل گروه دهند، در مسیریاب‌ها جداول کوچکتری جهت نگهداری اطلاعات مسیریابی این زیرشبکه‌ها نیاز است و این مسئله باعث کاهش سربار شبکه می‌گردد.
- در مجموع، موارد ذکرشده در بالا عملکرد مناسب‌تری برای شبکه فراهم می‌نمایند.

طراحان پروتکل IP، در ابتدا یک شبکه اینترنت کوچک متشکل از ده‌ها شبکه و هزاران میزبان را پیش‌بینی می‌کردند. بنابراین در طرح آدرس‌دهی آنها برای هر زیرشبکه فیزیکی یک آدرس شبکه

---

1. Subnetting
2. Subnet

استفاده می‌شد. اما رشد پیش‌بینی نشده اینترنت، تعداد زیادی از مشکلات را برای مسئولین و طراحان اینترنت ایجاد نمود که در ادامه دو مورد از آنها آورده شده است:

- کمبود آدرس‌ها: زمانی که یک سازمان قصد داشت از چندین شبکه فیزیکی استفاده کند، باید برای هر کدام از آنها یک آدرس شبکه درخواست می‌کرد. بنابراین با افزایش تعداد شبکه‌ها دیگر آدرسی جهت اختصاص به آنها وجود نخواهد داشت.
- جداول مسیریابی بزرگ: اگر هر مسیریاب در اینترنت نیازمند نگهداری اطلاعات مسیریابی هر شبکه فیزیکی باشد، جدول مسیریابی آن بطور غیر ممکنی افزایش خواهد یافت. این مسئله باعث ایجاد حجم طاقت فرسایی از سربار مدیریتی جهت نگهداری این جداول شده و در نتیجه سربار فیزیکی (مثل سربار CPU، فضای دیسک، حافظه و ... ) برای این مسیریاب‌ها به دنبال خواهد داشت. حال چون هر مسیریاب اطلاعات مسیریابی خود را با سایر مسیریاب‌ها تبادل می‌کند، ترافیک شبکه را افزایش داده و در نتیجه موجب کاهش عملکرد شبکه می‌گردد.

یکی ار راهکارهایی که جهت برخورد با این مشکلات استفاده می‌شود و در این کتاب نیز مورد بررسی قرار می‌گیرد استفاده از ساب‌نتینگ می‌باشد. در واقع به کمک ساب‌نتینگ می‌توان یک شبکه IP را بطور منطقی به زیرشبکه‌هایی تقسیم نمود. در قسمت بعد نحوه انجام این کار را شرح خواهیم داد.

## پیاده‌سازی سابنتینگ

قبل از اقدام به اجرای سابنتینگ در یک شبکه، باید نیازمندی‌های این کار و همچنین طرحی مناسب برای پیاده‌سازی آن مشخص نمایید. در ادامه این موارد را مورد بررسی قرار می‌دهیم.

### تعیین نیازمندی‌های سابنتینگ

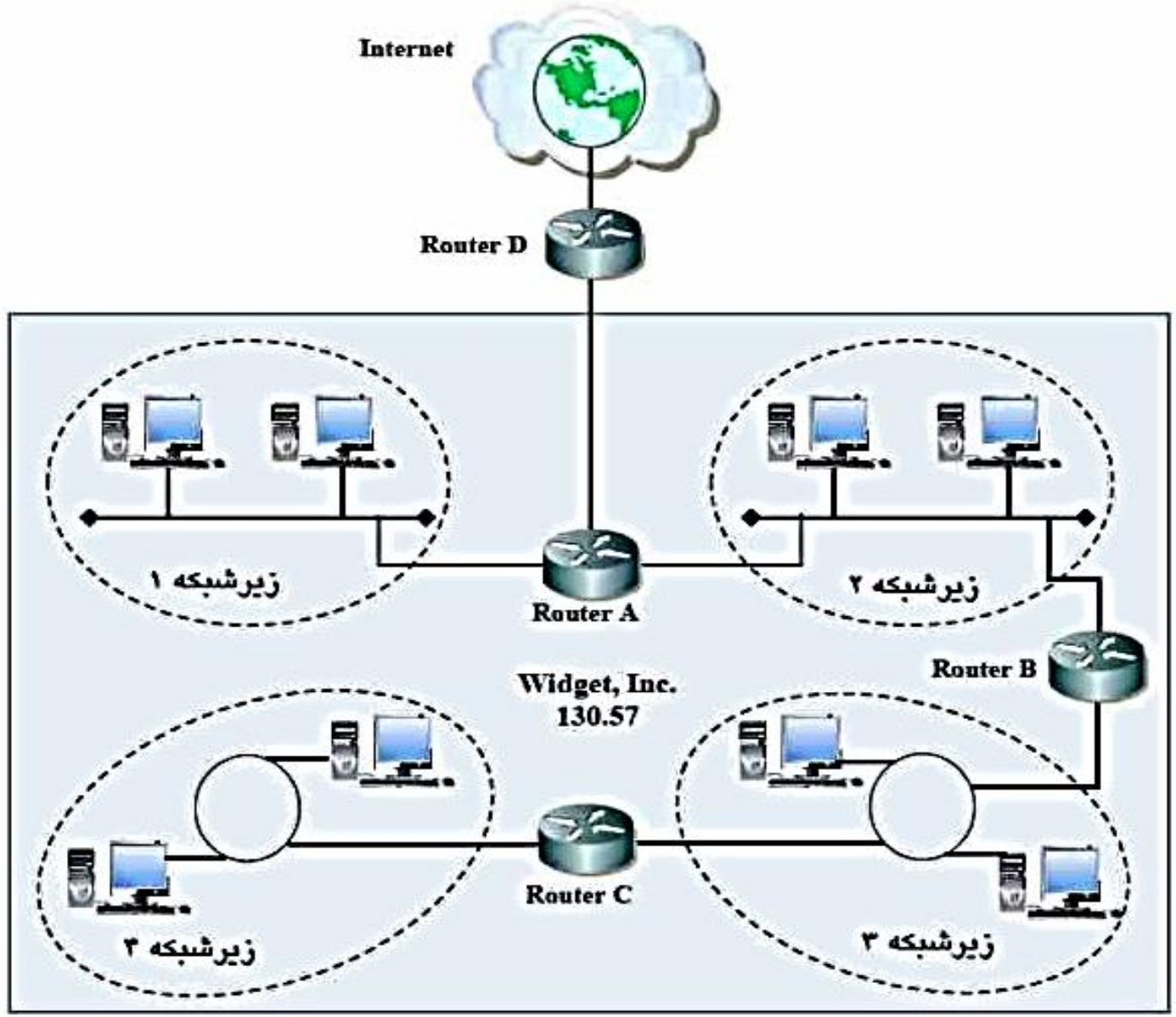
جهت تعیین نیازمندی‌های سابنتینگ، رهنمودهای زیر را دنبال کنید:

۱. شناسه شبکه (قاب زیرشبکه) را تعیین کنید. این شناسه با توجه به کلاسی که از آن استفاده می‌کنید مشخص می‌شود و برای همه میزبان‌ها مشترک خواهد بود.
۲. برای هر قسمت از شبکه (که به عنوان یک زیرشبکه در نظر گرفته می‌شود) شناسه‌ای متمایز مشخص کنید.
۳. به هر زیرشبکه ایجاد شده محدوده‌ای از شناسه‌ها را جهت شناسایی دستگاه‌های TCP/IP (شامل کامپیوترها، پرینترهای تحت شبکه و ...) اختصاص دهید.

### نحوه پیاده سازی سابنتینگ

جهت پیاده سازی سابنتینگ باید به همه ماشین‌ها در یک زیرشبکه فیزیکی، آدرس زیرشبکه

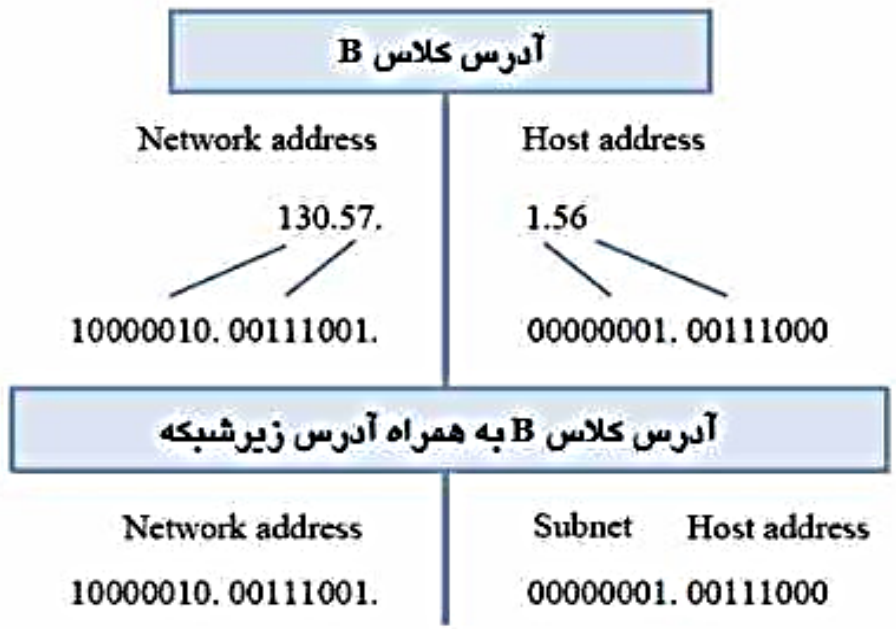
یکسانی اختصاص داده شود. به عنوان مثال در شکل زیر کلیه ماشین‌هایی که در زیرشبکه ۱ قرار دارند، باید دارای آدرس زیرشبکه ۱ باشند.



در هنگام پیاده‌سازی سابنتینگ، با توجه به کلاسی که جهت آدرس‌دهی انتخاب می‌شود، بخش شبکه از آدرس IP برای ماشین‌های موجود در همه زیرشبکه‌ها ثابت است. بنابراین نمی‌توان برای یک میزبان در این زیرشبکه‌ها آدرس شبکه را تغییر داد، مگر اینکه این آدرس برای همه میزبان‌ها تغییر کند (یا به عبارتی از آدرس دیگری استفاده شود). استفاده از آدرس شبکه یکسان موجب بهره‌مندی از حداکثر فضای آدرس‌دهی می‌گردد. همانطور که در شکل ۱-۱۳ مشاهده می‌کنید، همه میزبان‌های شرکت Widget دارای آدرس شبکه 130.57 می‌باشند بنابراین این آدرس برای همه آنها ثابت است. در واقع، طرح سابنتینگ به این صورت است که چون آدرس شبکه جهت شناسایی کل شبکه در یک

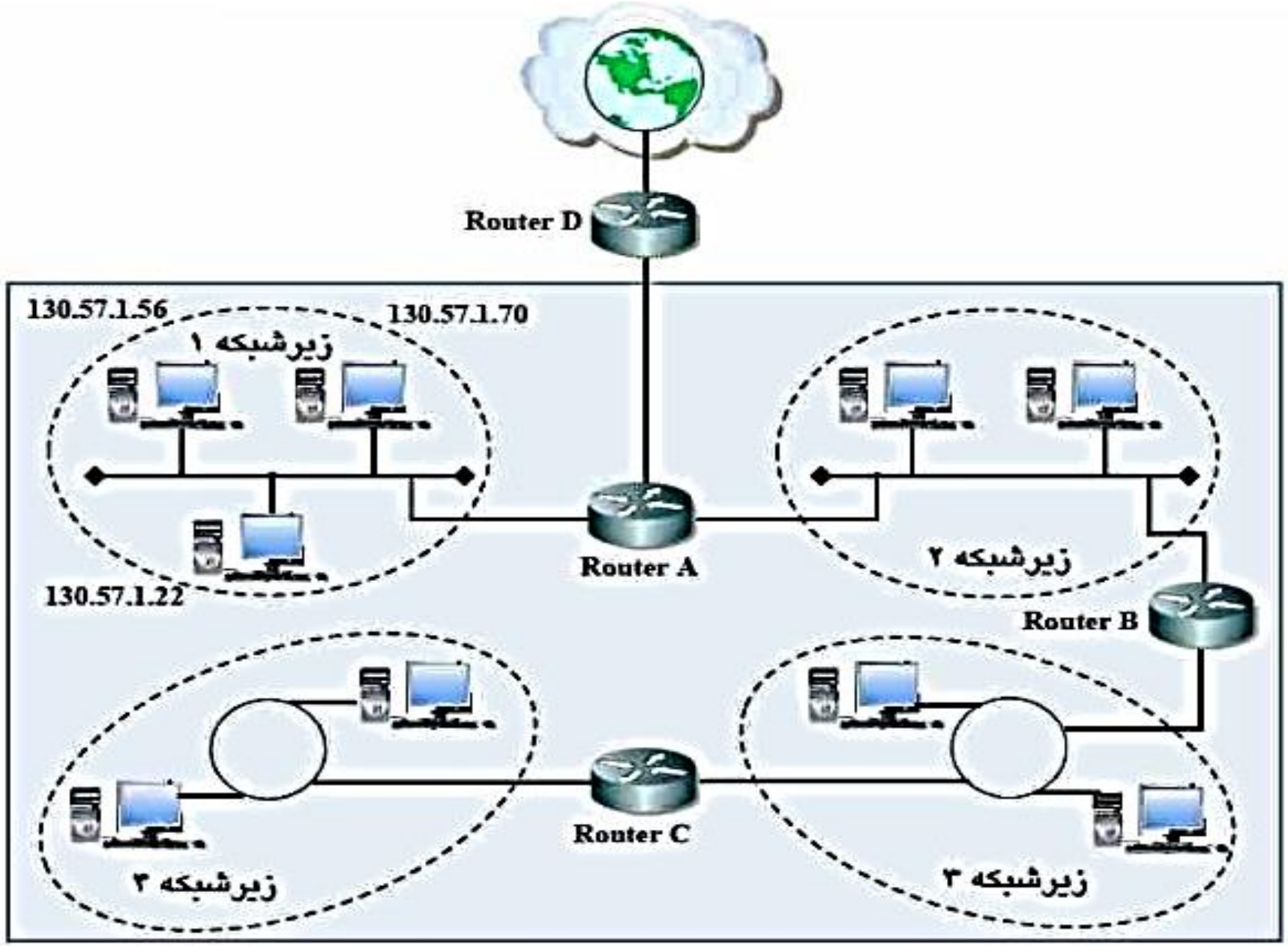
سازمان استفاده می‌شود بدون تغییر باقی می‌ماند اما با قرض‌گرفتن بیت‌های آدرس میزبان و در نتیجه ایجاد تغییر در بخش میزبان از آدرس، می‌توان زیرشبکه‌ها را ایجاد نموده و موقعیت قرارگیری میزبان‌ها در هر زیرشبکه را تعیین نمود.

در مثال بالا چون آدرس شبکه در شرکت Widget از کلاس B می‌باشد، دو بایت اول آدرس در همه ماشین‌ها صرفنظر از اینکه در چه زیرشبکه‌ای قرار دارند یکسان است. در اینجا بایت سوم از آدرس هر ماشین به آدرس زیرشبکه اختصاص داده می‌شود. به عنوان مثال مقدار بایت سوم در زیرشبکه ۱ دارای مقدار 00000001 می‌باشد. در این آدرس‌ها، مقدار چهارمین بایت (به همراه مقدار سومین بایت که تعیین‌کننده محل قرارگیری میزبان‌ها در هر زیرشبکه می‌باشد) برای هر میزبان باید منحصر بفرد باشد. در شکل زیر، نحوه استفاده آدرس شبکه و آدرس میزبان با یکدیگر نشان داده شده است.



## نحوه استفاده از قاب زیرشبکه

به منظور عملکرد صحیح طرح آدرس زیرشبکه، هر ماشین باید از وضعیت بیت‌های شبکه، زیرشبکه و میزبان‌ها آگاه باشد. این کار با اختصاص قاب زیرشبکه به هر میزبان امکان‌پذیر است. در این مثال، مدیر شبکه یک قاب زیرشبکه ۲۲ بیتی متشکل از بیت‌های ۰ و ۱ ایجاد می‌نماید. دنباله بیت‌های ۱ در قاب زیرشبکه، بیانگر آدرس شبکه و زیرشبکه در آدرس IP می‌باشند. بیت‌های صفر نیز آدرس میزبان را مشخص می‌نمایند. در شکل‌های ۱–۱۵ و ۱–۱۶ مثالی (از کلاس B) در این رابطه آورده شده است.


Router D
130.57.1.56
130.57.1.70
زیرشبکه ۱
130.57.1.22
Router A
زیرشبکه ۲
Router B
Router C
زیرشبکه ۳
زیرشبکه ۳

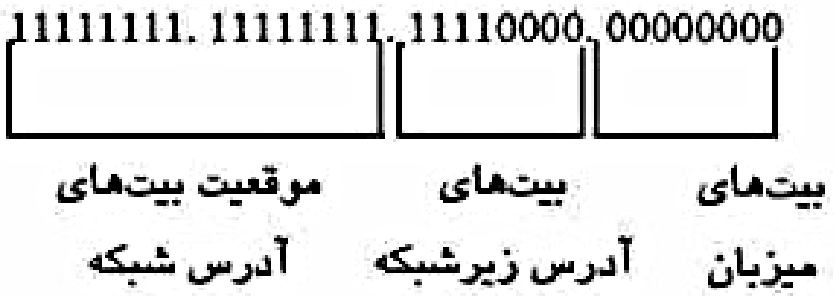
شکل ۱–۱۵

## وضعیت بیت‌ها

1ها: موقعیت‌هایی است که آدرس شبکه یا زیرشبکه را نشان می‌دهند.

0ها: موقعیت‌هایی است که آدرس میزبان را نشان می‌دهند.

## قاب زیرشبکه برای شرکت Widget




شکل ۱-۱۶

در مثال بالا دو بایت اول قاب زیرشبکه با بیت‌های ۱ مقداردهی شده است زیرا آدرس این شبکه

از نوع کلاس B بوده که دارای فرمت Network.Network.Host.Host می‌باشد. اگر بخاطر داشته باشید گفتیم جهت ایجاد زیرشبکه از بیت‌های میزبان استفاده می‌شود، بنابراین در اینجا بیت‌های موجود در بایت سوم به آدرس زیرشبکه اختصاص داده شده و با 11110000 که معادل شماره زیرشبکه ۲۲۰ می‌باشد مقداردهی شده است. در این مثال تنها چهارمین بایت به آدرس میزبان اختصاص داده شده است. توجه داشته باشید که ممکن است تعداد بیت‌های اختصاص داده شده به زیرشبکه و میزبان‌ها کمتر یا بیشتر از این مقدار باشد (مثلاً دو بیت، سه بیت و یا ... ). در طول فصل با این موارد نیز آشنا خواهید شد.

قاب زیرشبکه را می‌توان با استفاده از معادل ده‌دهی (مبنای ده) بیت‌ها نیز نشان داد. الگوی دودویی 11110000 معادل عدد ۲۲۰ می‌باشد. بنابراین قاب زیرشبکه در مثال قبل می‌تواند به دو طریق زیر نشان داده شود:

قاب زیرشبکه بصورت دودویی: 11111111. 11111111. 11110000. 00000000

قاب زیرشبکه بصورت ده‌دهی: 255 . 255 . 220 . 0

در همه زیرشبکه‌ها نیاز به استفاده از قاب‌های زیرشبکه سفارشی (قاب‌هایی که مقادیر اکتت‌های مربوط به زیرشبکه در آن عددی غیر از ۲۵۵ باشد) نمی‌باشد، بلکه می‌توان از همان مقادیر پیش‌فرض قاب زیرشبکه استفاده نمود. به عبارتی می‌توان در مورد این شبکه‌ها اینگونه تصور کرد که فاقد آدرس زیرشبکه می‌باشند. در جدول ۱-۳ مقادیر مختلف قاب زیرشبکه برای سه کلاس A، B و C (زمانی که هیچ تغییری در تعداد بیت‌های آن ایجاد نشده) آورده شده است.

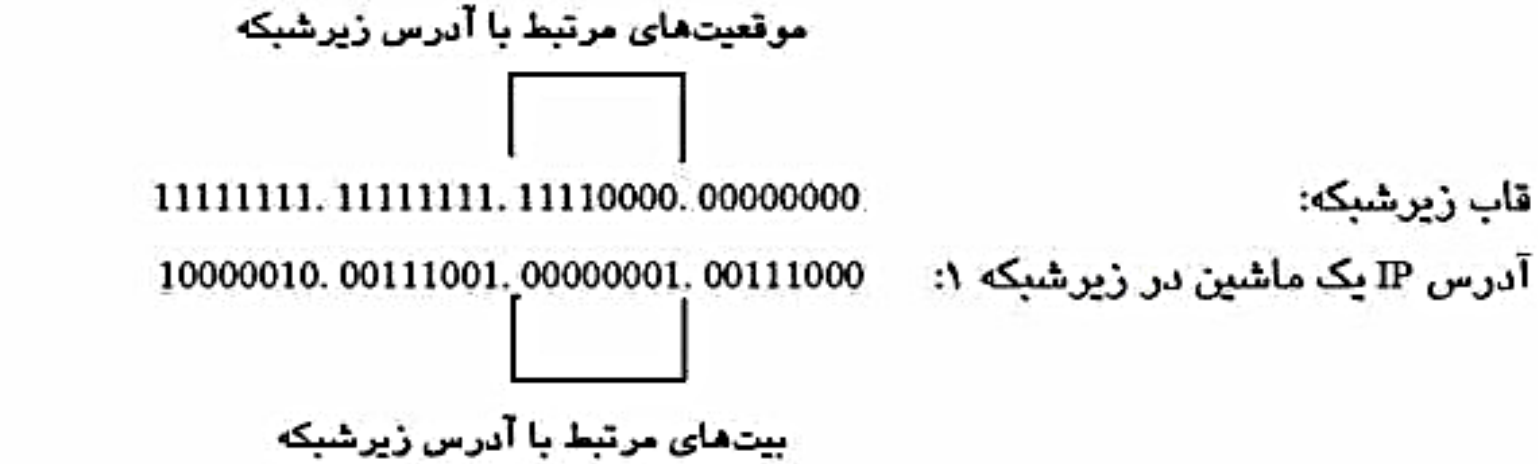
جدول ۱-۳: قاب زیرشبکه برای سه کلاس A، B و C

| کلاس | فرمت | قاب زیرشبکه پیش‌فرض |
|---|---|---|
| A | Network.Host.Host.Host | 255.0.0.0 |
| B | Network.Network.Host.Host | 255.255.0.0 |
| C | Network.Network. Network.Host | 255.255.255.0 |

پس از ایجاد قاب زیرشبکه، آدرس IP باید از محل قرارگیری خود در زیرشبکه آگاه گردد. این کار با اعمال قاب زیرشبکه برروی آدرس مورد نظر (توسط نرم افزار IP) انجام می‌شود. در واقع بیت‌هایی از آدرس IP که متناظر با بیت‌های تعیین‌کننده زیرشبکه در قاب زیرشبکه هستند، محل قرارگیری میزبان در زیرشبکه را مشخص می‌نمایند. برای روشنتر شدن این موضوع، در شکل ۱-۱۷ مثالی از آدرس IP و قاب زیرشبک آن آورده شده است.

1ها: موقعیت‌هایی است که آدرس شبکه یا زیرشبکه را نشان می‌دهند.

0ها: موقعیت‌هایی است که آدرس میزبان را نشان می‌دهند.




شکل ۱-۱۷

در این مثال، نرم افزار IP تشخیص می‌دهد که بایت سوم از قاب زیرشبکه به‌جای آدرس میزبان، برای آدرس زیرشبکه استفاده شده است. بنابراین به موقعیت بیت‌های متناظر با این بایت درآدرس IP که دارای مقدار 00000001 می‌باشد نگاه می‌کند.

در مرحله آخر نیز باید شماره زیرشبکه تعیین گردد. این کار با تبدیل مقادیر دودویی بایت سوم از آدرس IP به معادل ده‌دهی آن انجام می‌شود که در شکل زیر قابل مشاهده می‌باشد.

## تبدیل دودویی به معادل ده‌دهی آن

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| موقعیت/مقدار: | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |
| سومین بایت در مثال Widget: | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| معادل ده‌دهی: | 1 | (1 = 1*1 + 2*0 + 4*0 + 8*0 + 16*0 + 32*0 + 64*0 + 128*0) | | | | | | |
| آدرس زیرشبکه: | 1 | | | | | | | |

شکل ۱–۱۸

زمانی‌که در مواردی مانند مثال قبل، بایت سوم را به عنوان آدرس زیرشبکه قرار می‌دهید، به سادگی می‌توانید آدرس زیرشبکه برای میزبان‌ها را مشخص نمایید. به عنوان مثال اگر شرکت Widget قصد داشته باشد زیرشبکه‌ای با شماره ٦ داشته باشد، سومین بایت از همه ماشین‌ها در زیرشبکه برابر با مقدار 00000110 (معادل دودویی عدد ٦) خواهد بود. علاوه بر این، استفاده از همه

بیت‌های یک بایت جهت اختصاص به آدرس شبکه، تعداد نسبتاً مناسبی از آدرس‌های زیرشبکه را برای شما فراهم می‌نماید، زیرا این بایت تعداد ۸ موقعیت از بیت‌ها که هرکدام می‌تواند مقدار ۰ یا ۱ داشته باشد را در اختیار شما قرار می‌دهد؛ بنابراین طبق رابطه ۲۵۶ = $۲^{۸}$، تعداد ۲۵۶ زیرشبکه قابل اختصاص در این کلاس (B) موجود می‌باشد. پس در نهایت شرکت Widget می‌تواند مجموعاً ۲۵۶ زیرشبکه و هر کدام با ۲۵۴ میزبان در اختیار داشته باشد.

اگرچه استاندارد RFC 950 استفاده از آدرس‌های زیرشبکه که تمام بیت‌های آن ۰ و یا تماماً ۱ باشد را ممنوع کرده است ولی امروزه اکثر محصولات امکان استفاده از آنها را فراهم می‌نمایند که از جمله آنها می‌توان به پشته‌های TCP/IP در محصولات مایکروسافت و همچنین نرم افزار بیشتر مسیریاب‌ها اشاره نمود. به هر حال تا حصول اطمینان از اینکه نرم‌افزار شبکه شما این دو آدرس را به رسمیت می‌شناسد، نباید از آنها استفاده نمایید.

### محاسبه تعداد زیرشبکه‌ها

فرمول‌هایی که برای محاسبه حداکثر تعداد زیرشبکه‌ها و حداکثر تعداد میزبان‌ها در هر زیرشبکه استفاده می‌شوند بصورت زیر می‌باشد:

حداکثر تعداد زیرشبکه‌ها: $۲^{\text{(تعداد بیت‌های ماسک شده (۱) در قاب زیرشبکه)}}$

حداکثر میزبان‌ها در هر زیرشبکه: $۲^{\text{(تعداد بیت‌های ماسک نشده ( ) در قاب زیرشبکه)}} - ۲$