شبکه‌های کامپیوتری

مسعود صبائی

دانشکده مهندسی کامپیوتر

دانشگاه صنعتی امیرکبیر

لایه شبکه – صفحه داده

لایه شبکه – صفحه داده

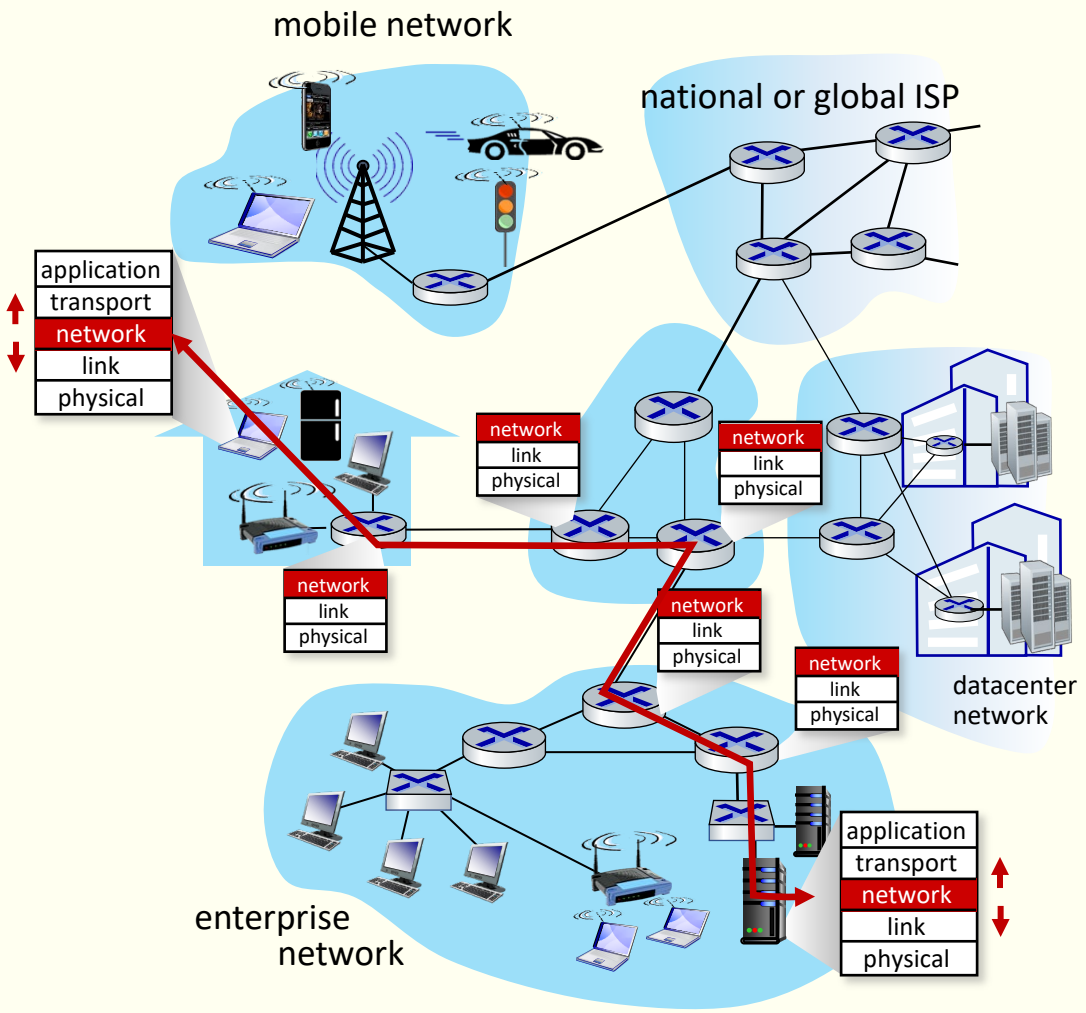
فهرست مطالب:

- معرفی وظایف لایه شبکه (مسیریابی و جلورانی)
- جلورانی (Forwarding)
  - صفحه داده و صفحه کنترل (شبکه‌سازی متداول و SDN)
  - شبکه‌های داده‌نگار و مدار مجازی
  - معماری مسیریاب
  - پروتکل اینترنت
    - فرمت بسته‌ها
    - آدرس‌دهی در اینترنت
    - پروتکل پیکربندی پویای میزبان (DHCP)
    - تبدیل آدرس شبکه (NAT)
    - خُردسازی و بازسازی بسته‌های IP
    - پروتکل IPv6

لایه شبکه – صفحه داده

پروتکل‌ها و سرویس‌های لایه شبکه

- انتقال سگمنت‌ها از گره میزبان فرستنده به گره میزبان گیرنده
- پروتکل‌های لایه شبکه در همه دستگاه‌های اینترنت هستند: میزبان‌ها، مسیریاب‌ها و ...
- گره میزبان فرستنده:
  - دریافت سگمنت‌ها از لایه بالاتر
  - قراردادن سگمنت‌ها را درون بسته‌ها
  - تحویل بسته‌ها به لایه پیوند داده برای انتقال به گره بعدی
- گره میزبان گیرنده:
  - دریافت بسته‌ها از لایه پیوند داده
  - بررسی فیلدهای سرآیند
  - تحویل سگمنت به پروتکل لایه بالاتر
- مسیریاب‌های میانی:
  - دریافت بسته‌های عبوری از لایه پیوند داده
  - بررسی فیلدهای سرآیند بسته‌ها
  - مشخص کردن پورت خروجی بسته‌ها بر روی مسیر انتها به انتها
  - انتقال بسته‌ها از پورت ورودی به پورت خروجی مشخص‌شده
  - تحویل بسته‌ها به لایه پیوند داده برای انتقال به گره بعدی روی مسیر



لایه شبکه – صفحه داده

دو وظیفه اصلی لایه شبکه

مسیریابی (routing):

- تعیین مسیر از گره مبدأ به گره مقصد (از پیش و قبل از انتقال‌ها باید انجام شود)
- الگوریتم‌های مسیریابی
- ایجاد جدول‌های جلورانی (forwarding table)

جلورانی (forwarding):

- هدایت بسته بر روی مسیر تعیین‌شده در جدول جلورانی
- انتقال بسته از لینک ورودی مسیریاب به لینک خروجی مناسب مسیریاب

مقایسه با سفر:

- مسیریابی: فرایند برنامه‌ریزی سفر (تعیین مسیر) از مبدأ به مقصد (قبل از شروع سفر)
- جلورانی: فرایند عبور از تقاطع‌ها (تعیین خروجی مناسب تقاطع روی مسیر)

forwarding

routing

لایه شبکه – صفحه داده

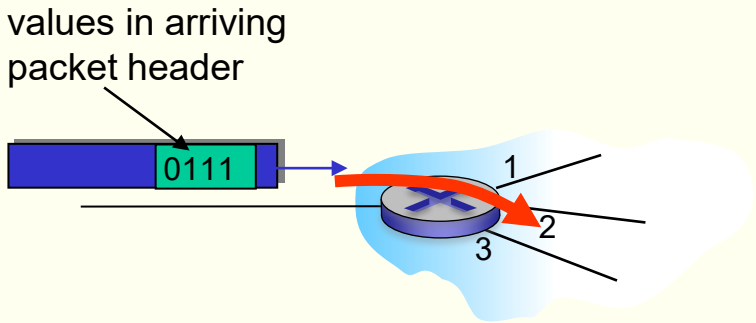
لایه شبکه: صفحه داده (data plane) و صفحه کنترل (control plane)

صفحه داده:

- وظیفه محلی در هر مسیریاب
- دریافت بسته از پورت ورودی
- تعیین پورت خروجی مناسب (با مراجعه به جدول جلورانی)
- انتقال بسته به پورت خروجی
- ارسال بسته بر روی رسانه فیزیکی

صفحه کنترل:

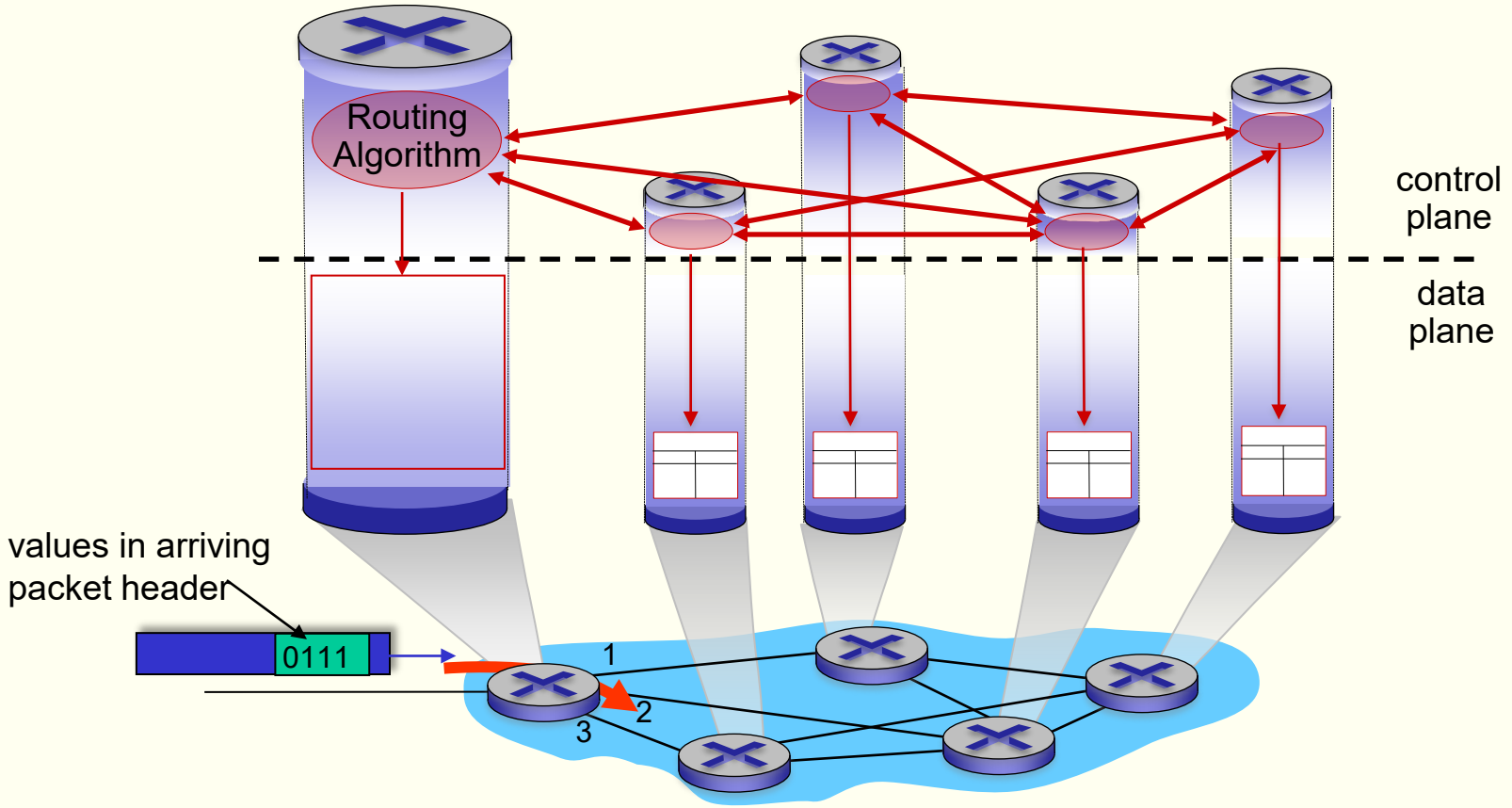
- وظیفه در سطح شبکه (سراسری)
- تعیین مسیریاب‌هایی که بسته از گره مبدأ عبور کند تا گره مقصد برسد (تعیین مسیر).
- دو رویکرد پیاده‌سازی صفحه کنترل:
- رویکرد سنتی (traditional): پیاده‌سازی توزیع‌شده درون مسیریاب‌ها
- رویکرد شبکه‌سازی نرم‌افزار محور (software defined networking): پیاده‌سازی متمرکز و نرم‌افزاری در سرورها (راه دور)



لایه شبکه – صفحه داده

صفحه کنترل به ازای هر مسیریاب:

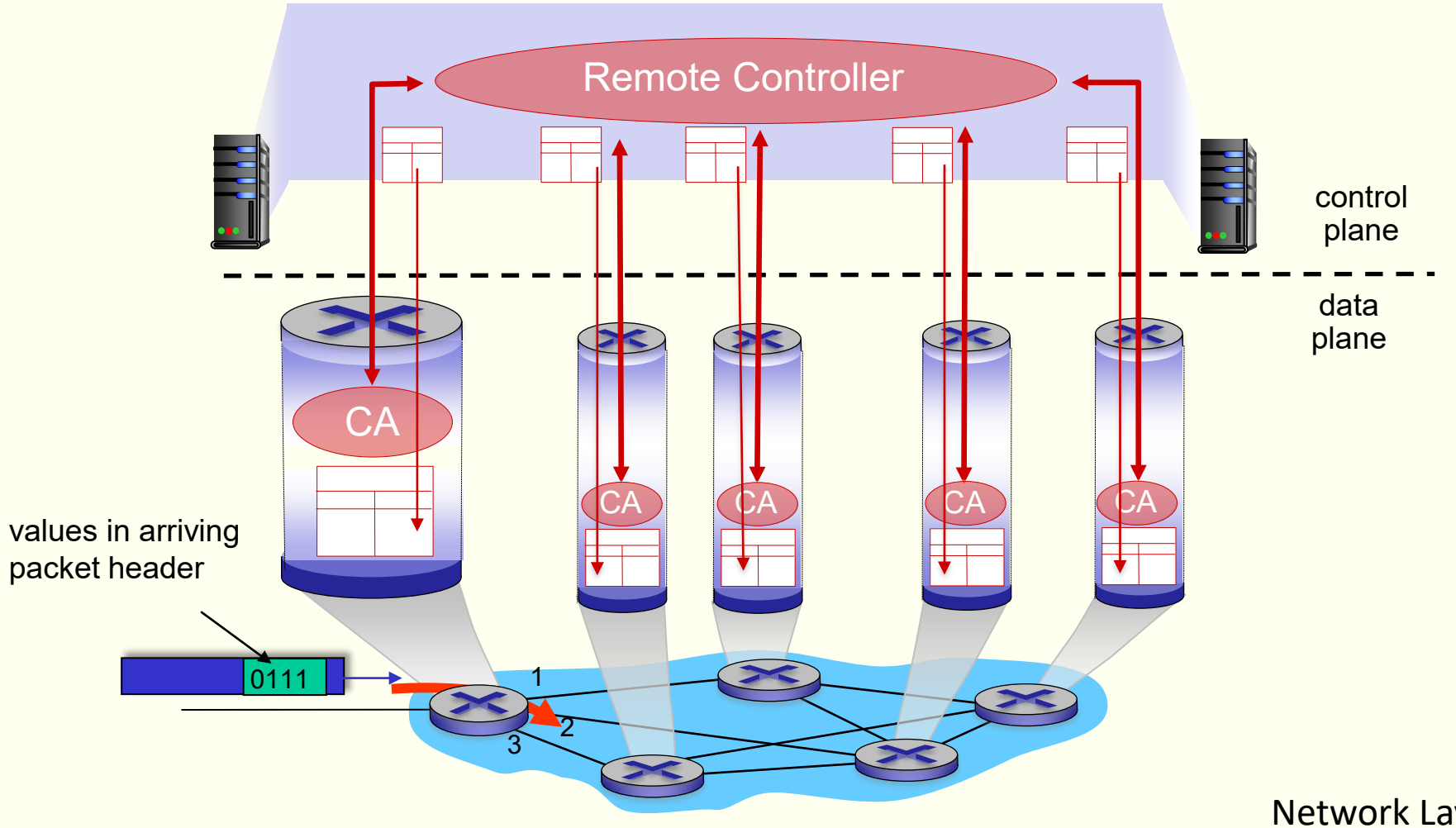
- جزءهای الگوریتم مسیریابی مجزا در مسیریاب‌ها در صفحه کنترل قرار دارند.
- این جزءهای الگوریتم مسیریابی برای انجام مسیریابی و ایجاد جدول‌های جلورانی محلی با هم در تعامل هستند (ارسال و دریافت اطلاعات مسیریابی)



لایه شبکه – صفحه داده

صفحه کنترل شبکه‌سازی نرم‌افزار محور (SDN):

- کنترل‌کننده راه‌دور، جدول‌های جلورانی را محاسبه کرده و درون مسیریاب‌ها قرار می‌دهد.



Network Layer: 4-7

مدل‌های سرویس لایه شبکه:

سرویس بدون اتصال: سویچینگ بسته‌ای بدون اتصال (شبکه‌های دیتاگرام)
connectionless packet switching (datagram networks)

عملکرد:

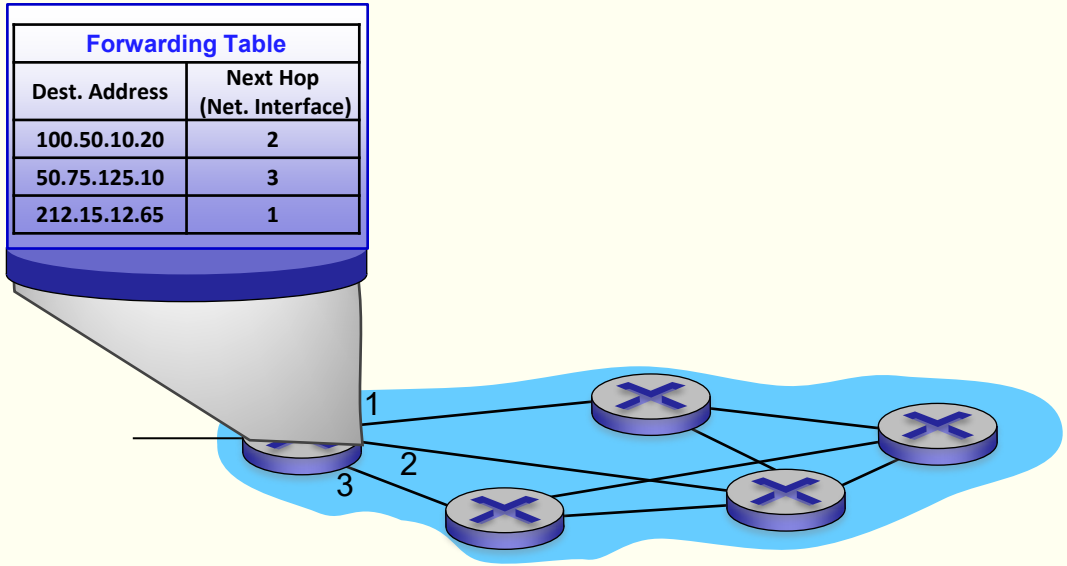
- ارسال بسته‌ها بدون نیاز به برقراری اتصال
- انجام مسیریابی و ایجاد جدول‌های جلورانی از قبل
- جلورانی بسته‌ها بر اساس آدرس مقصد
- سادگی پیاده‌سازی

ویژگی‌ها:

- عدم تحویل تضمینی
- عدم تضمین حداکثر تأخیر
- عدم تضمین حفظ ترتیب ارسال بسته‌ها
- عدم تضمین حداقل پهنای‌باند

نمونه:

- شبکه اینترنت



مدل‌های سرویس لایه شبکه:

سرویس اتصال‌گرا: سویچینگ بسته‌ای اتصال‌گرا (شبکه‌های مدارمجازی)
connection-oriented packet switching (virtual circuit networks)

عملکرد:

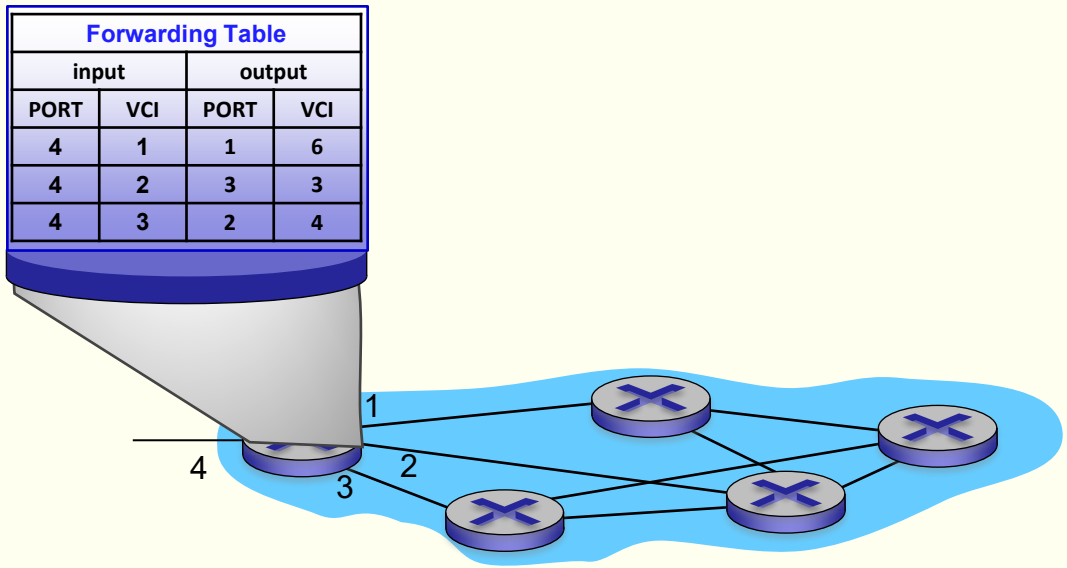
- پیدا کردن مسیر، برقراری اتصال و اضافه کردن یک سطر به جدول جلورانی در هر یک از سوییچ‌های مسیر، قبل از ارسال بسته‌ها
- استفاده از اندیس جدول جلورانی به عنوان شناسه مسیر مجازی (virtual circuit identifier - VCI)
- عبور همه بسته‌ها از یک مسیر
- جلورانی بسته‌ها بر اساس شناسه مدار مجازی (VCI)
- پیاده‌سازی پیچیده‌تر نسبت به دیتاگرام

ویژگی‌ها:

- امکان تحویل تضمینی
- امکان تضمین حداکثر تأخیر
- تضمین حفظ ترتیب ارسال بسته‌ها
- امکان تضمین حداقل پهنای‌باند

نمونه:

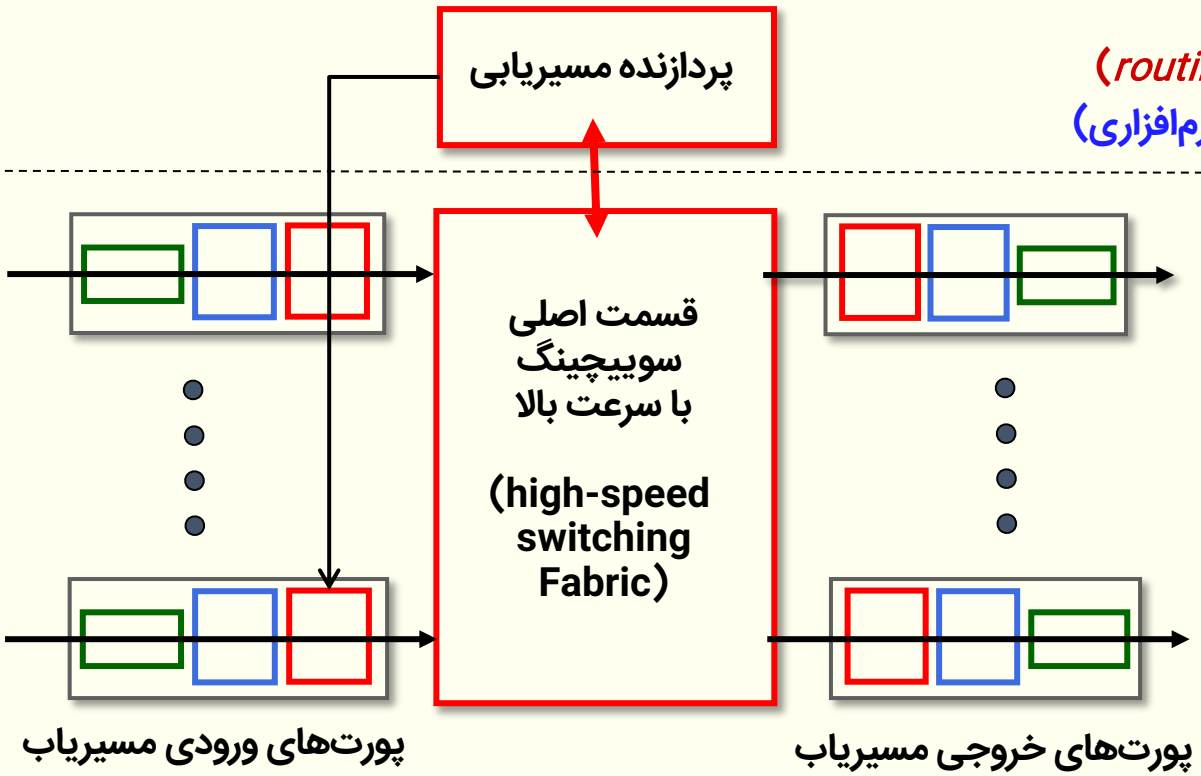
- شبکه ATM (Asynchronous Transfer Mode)
- شبکه Frame Relay



لایه شبکه – صفحه داده

معماری مسیریاب:

معماری سطح بالای یک مسیریاب نمونه



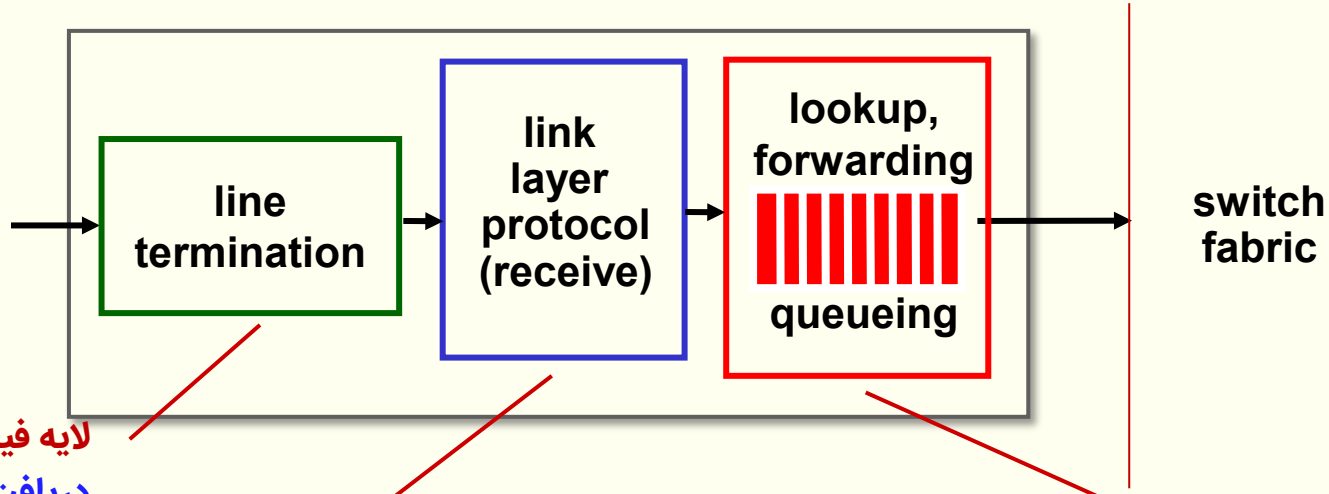
صفحه کنترل مسیریابی و مدیریت
(*routing, management control plane*)
انجام عملیات در بازه زمانی میلی‌ثانیه (نرم‌افزاری)

صفحه جلورانی داده
(*forwarding data plane*)
انجام عملیات جلورانی در بازه زمانی نانوثانیه (سخت‌افزار)

لایه شبکه – صفحه داده

معماری مسیریاب:

وظایف پورت‌های ورودی:



لایه فیزیکی:
دریافت در سطح بیت

لایه پیوند داده:
دریافت رشته بیت (bit stream)

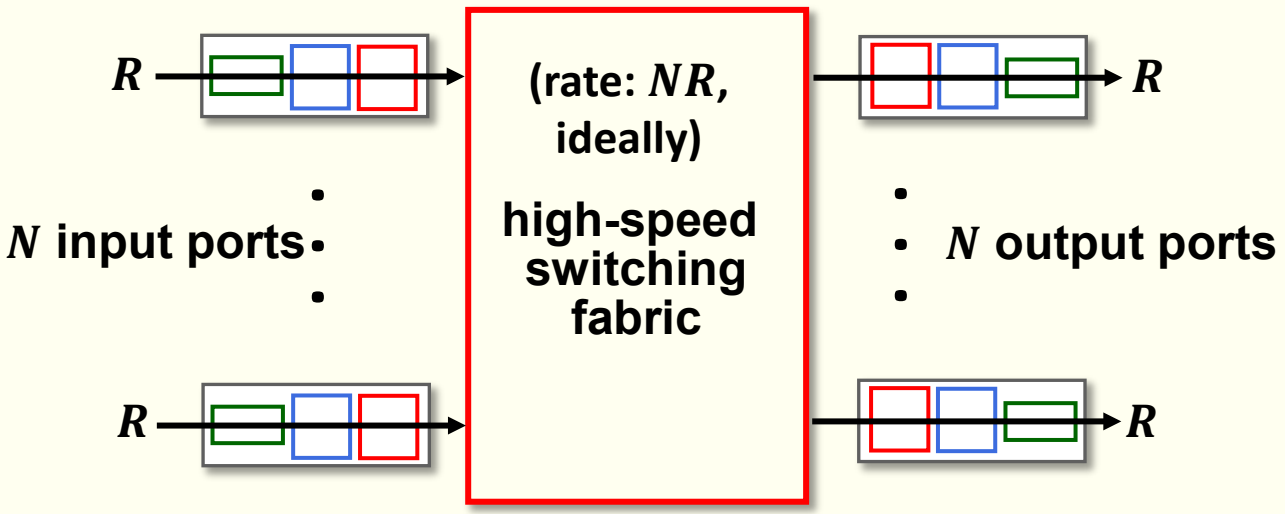
سوییچینگ غیرمتمرکز:

- بررسی فیلدهای سرآیند، تعیین شماره پورت خروجی با جستجوی در جدول جلورانی
- انجام پردازش پورت‌های ورودی با سرعت دریافت خط
- استفاده از بافرهای ورودی، بدلیل اینکه ممکن است سرعت دریافت (لحظه‌ای) بسته‌ها بیشتر از سرعت قسمت اصلی سوییچینگ باشد.
- **جلورانی بر اساس آدرس مقصد:** جلورانی فقط بر اساس فیلد آدرس IP انجام می‌شود (سنتی).
- **جلورانی تعمیم‌یافته:** جلورانی بر اساس مجموعه‌ای از مقادیر فیلدهای سرآیندها انجام می‌شود.

معماری مسیریاب:

قسمت اصلی سوییچینگ (switch fabric): انتقال بسته‌ها از لینک ورودی به لینک خروجی مناسب

- نرخ سوییچینگ: سرعت (حداکثری) انتقال بسته‌ها را از ورودی‌ها به خروجی‌ها
  - چندین برابر نرخ ورودی/خروجی
  - نرخ سوییچینگ مطلوب: با N ورودی، N برابر نرخ خط



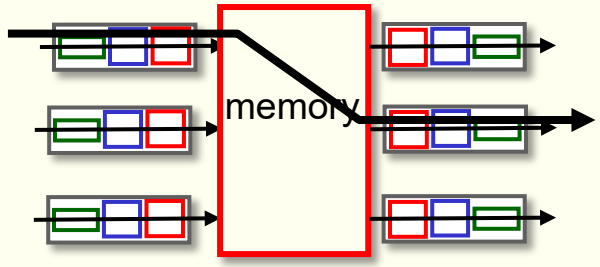
لایه شبکه – صفحه داده

معماری مسیریاب:

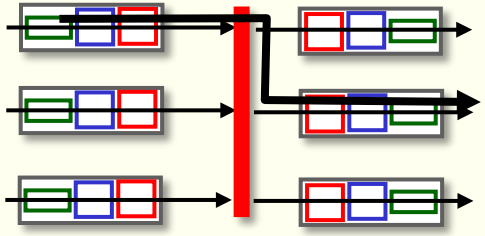
قسمت اصلی سوییچینگ (switch fabric): انتقال بسته‌ها از لینک ورودی به لینک خروجی مناسب

- نرخ سوییچینگ: سرعت (حداکثری) انتقال بسته‌ها را از ورودی‌ها به خروجی‌ها
  - چندین برابر نرخ ورودی/خروجی
  - نرخ سوییچینگ مطلوب: با N ورودی، N برابر نرخ خط

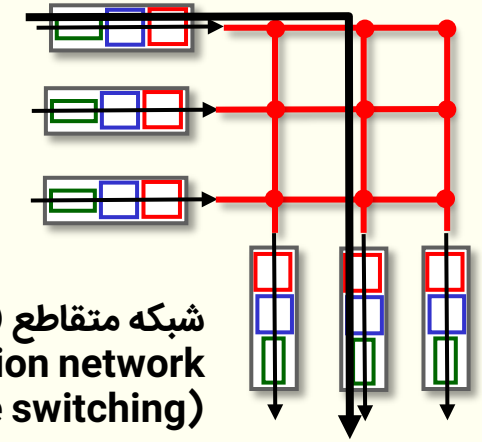
- سه نوع اصلی از قسمت اصلی سوییچینگ:



حافظه مشترک



گذرگاه (باس) مشترک

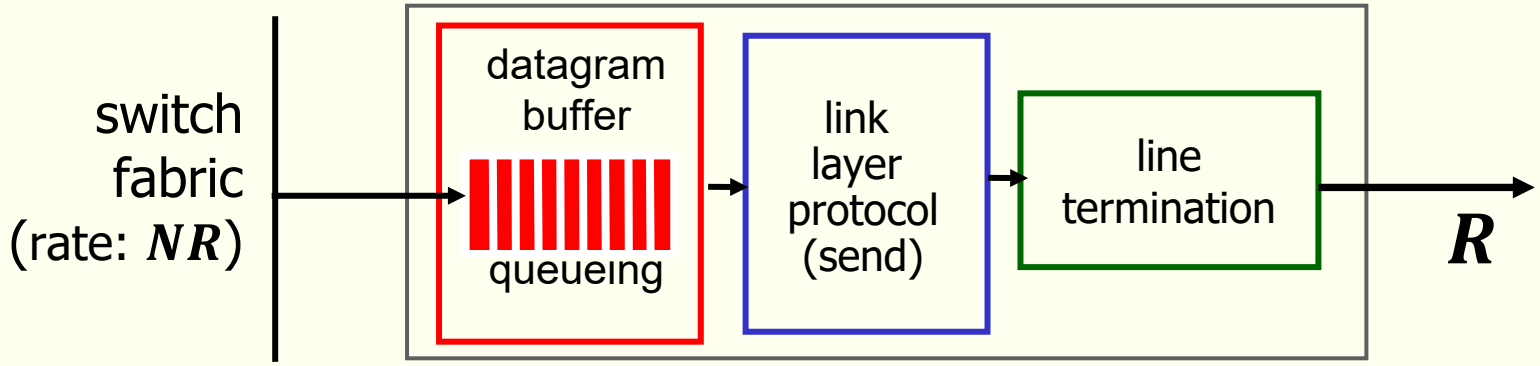


شبکه متقاطع (سوییچینگ فضایی)
interconnection network
(space switching)

لایه شبکه – صفحه داده

معماری مسیریاب:

وظایف پورت‌های خروجی:



- **بافر کردن بسته‌ها در پورت خروجی:**
  - بدلیل اینکه ممکن است سرعت (لحظه‌ای) سوییچینگ بیشتر از نرخ خروجی باشد وجود بافر در پورت‌های خروجی لازم است.
  - خط مشی (مدیریت بافر) حذف بسته در صورت نبود فضای خالی در بافر

بسته‌ها به دلیل ازدحام و نبود فضای خالی در بافرها ممکن است حذف شوند.

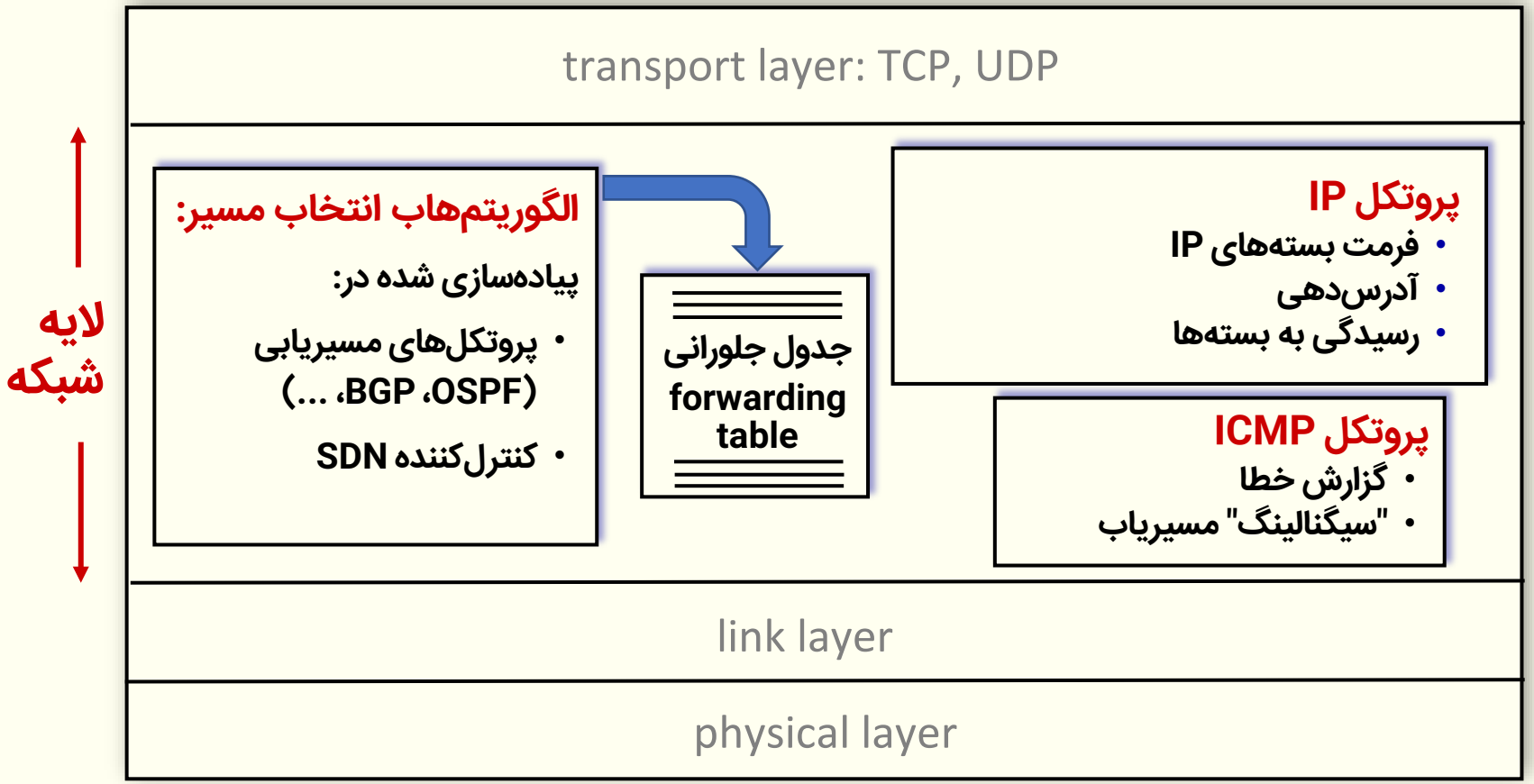
- نظام نوبت‌بندی (scheduling) برای انتخاب بسته از بافر برای ارسال روی لینک خروجی

الویت نوبت‌بندی- کدام (پورت یا جریان) کارآیی بهتری دریافت می‌کند. (عدالت در شبکه)

لایه شبکه – صفحه داده

لایه شبکه اینترنت

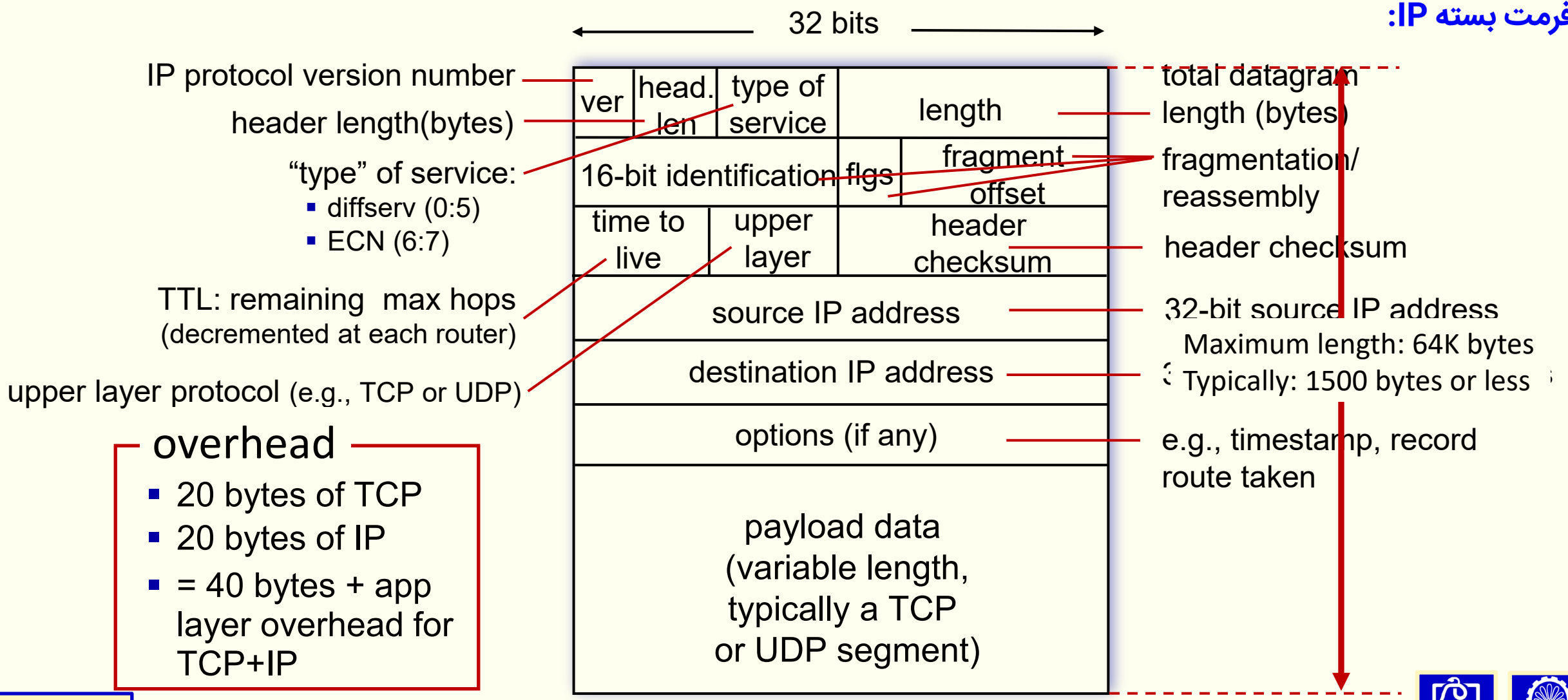
وظایف لایه شبکه در میزبان‌ها و مسیریاب‌ها:



لایه شبکه – صفحه داده

پروتکل اینترنت (IP):

فرمت بسته IP:



overhead

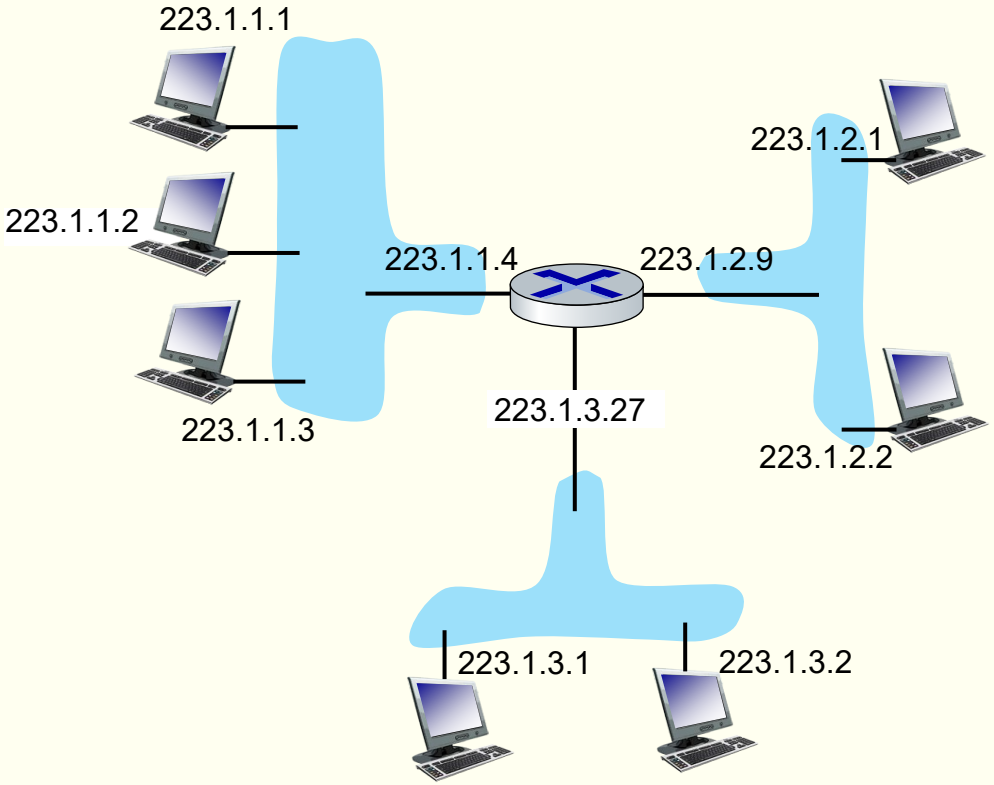
- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead for TCP+IP

لایه شبکه – صفحه داده

پروتکل اینترنت (IP):

آدرس‌دهی:

- آدرس IP یک شناسه ۳۲ بیتی است که به هر واسط شبکه کامپیوترهای میزبان یا مسیریاب‌ها اختصاص داده می‌شود.
- واسط شبکه (کارت شبکه): اتصال دهنده کامپیوتر میزبان یا مسیریاب به رسانه فیزیکی
- وظایف واسط شبکه: لایه پیوند داده و لایه فیزیکی
- مسیریاب‌ها غالباً چند واسط شبکه دارند.
- کامپیوترهای میزبان غالباً یک یا دو واسط شبکه دارند (واسط شبکه سیمی اترنت و واسط شبکه بی‌سیم 802.11)



dotted-decimal IP address notation:

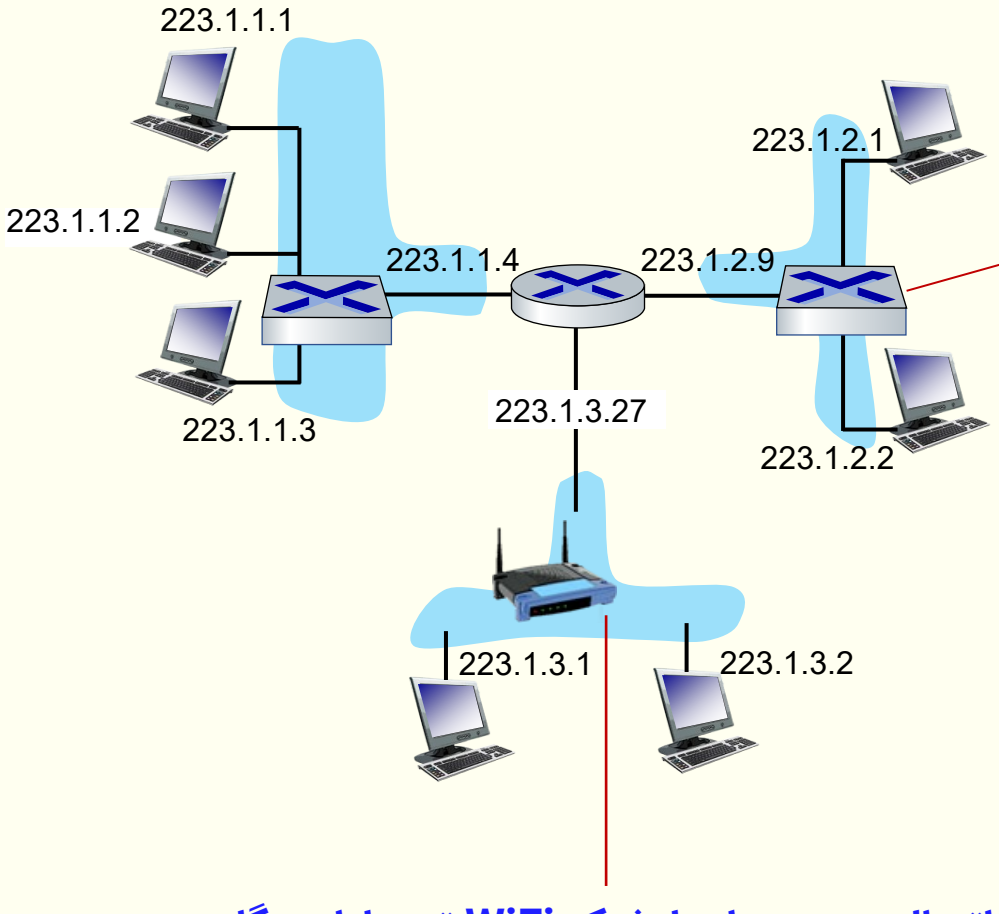
223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

لایه شبکه – صفحه داده

پروتکل اینترنت (IP):

اتصال از طریق واسط شبکه:



اتصال سیمی واسط شبکه اترنت توسط سوییچ اترنت (Ethernet Switch)

اتصال بی‌سیم واسط شبکه WiFi توسط ایستگاه پایه WiFi (Access Point)

- نحوه کار وسط شبکه در فصل‌های ۶ و ۷ کتاب مرجع آمده است (موضوع درس انتقال داده‌ها).
- نگران نحوه عملکرد واسط شبکه نباشید، به صورت منطقی فرض کنید که یک واسط شبکه یک گذرگاه (باس) منطقی است.

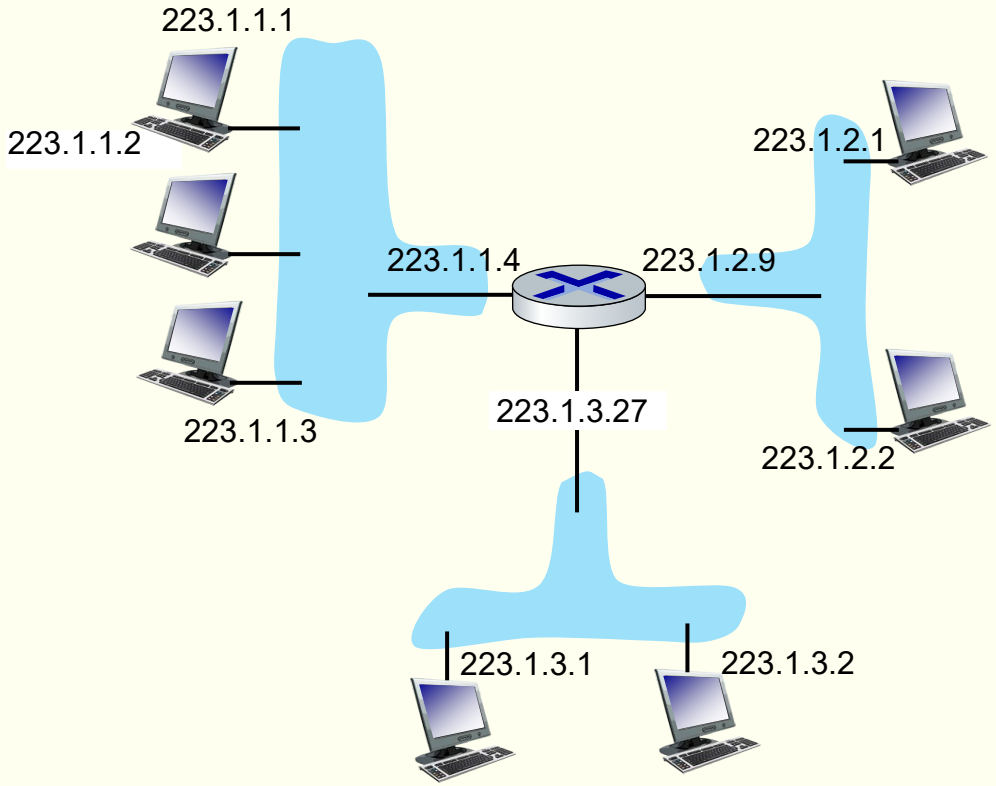
پروتکل اینترنت (IP):

زیرشبکه‌ها (subnets):

- تمام دستگاه‌های (کامپیوترهای میزبان یا مسیریاب‌ها) که مستقیماً از طریق یک واسط شبکه به هم متصل شده‌اند، یک زیر شبکه را تشکلیل می‌دهند.
- آدرس‌های IP دستگاه‌ها متعلق به یک زیر شبکه پشت سرهم هستند.
- آدرس IP به دو بخش تقسیم می‌شود:
  - بخش زیرشبکه: بیت‌های با ارزش آدرس IP که برای تمام دستگاه‌های یک زیرشبکه یکسان هستند.
  - بخش میزبان: باقیمانده بیت‌های کم ارزش آدرس IP که یک دستگاه داخل یک زیر شبکه را مشخص می‌کند.

(sub)net ID	host ID

- هر زیر شبکه یک محدوده آدرس دارد.



شبکه با سه زیرشبکه

لایه شبکه – صفحه داده

پروتکل اینترنت (IP):

زیرشبکه‌ها (subnets):

- نحوه تعریف زیر شبکه‌ها:

۱. همه واسط‌های شبکه را کامپیوترهای میزبان و مسیریاب‌ها جدا کنید. شبکه به جزیره‌هایی از شبکه‌های جزیره‌ای تبدیل می‌شود.

۲. هر شبکه جزیره‌ای یک زیرشبکه (subnet) است.

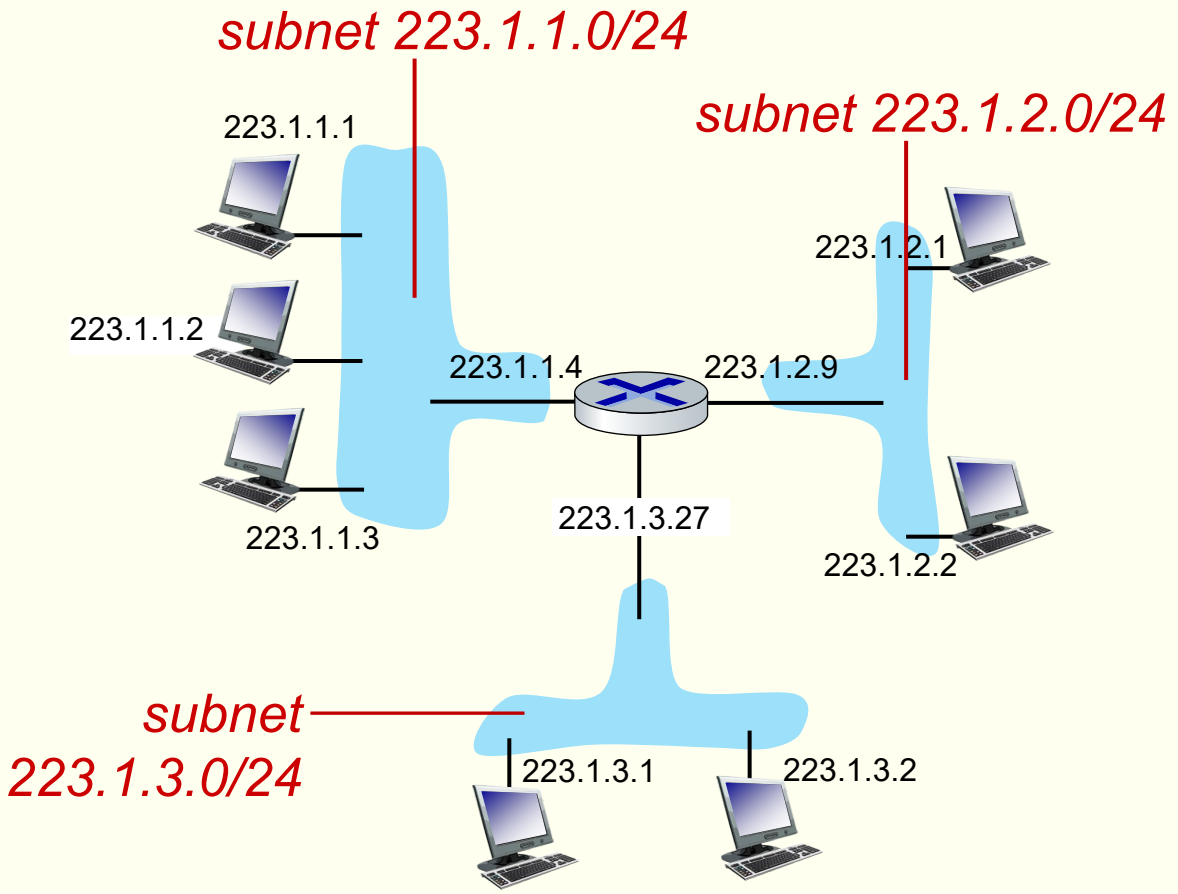
۳. هر زیرشبکه با یک آدرس تعریف می‌شود. این آدرس شامل ۳۲ بیت آدرس IP و ۳۲ بیت ماسک زیر شبکه (subnet mask) است.

- ۳۲ بیت آدرس IP شامل بخش subnet ID است و بخش host ID آن تماماً صفر است.
- ۳۲ بیت ماسک زیرشبکه از بیت با ارزش به تعداد بیت‌های subnet ID بیت‌های یک است و بقیه بیت‌ها صفر است.
- مثال:

IP address: 223.1.1.0
subnet mask: 255.255.255.0

یا

IP address & subnet mask: 223.1.1.0/24

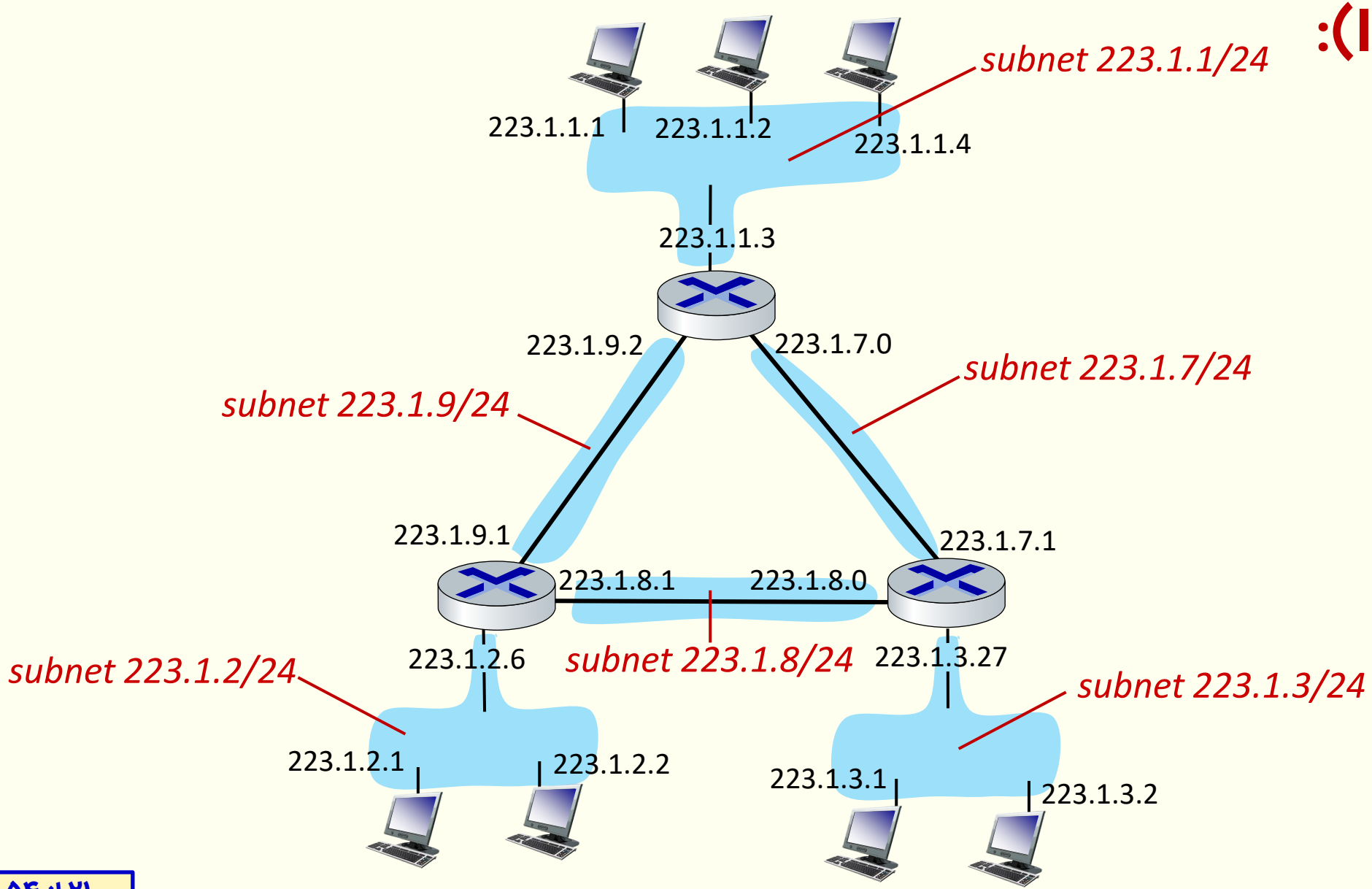


لایه شبکه – صفحه داده

پروتکل اینترنت (IP):

زیرشبکه‌ها (subnets):

- نحوه تعریف زیر شبکه‌ها:
- مثال:

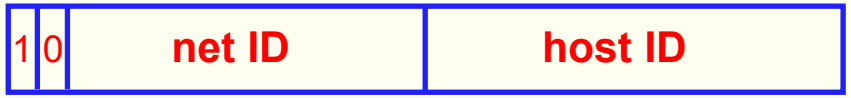


پروتکل اینترنت (IP):

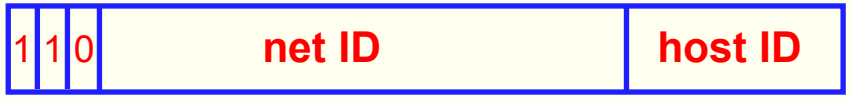
آدرس‌دهی IP: مسیریابی بین دامنه‌ای بدون طبقه‌بندی (CIDR – Classless Inter-Domain Routing):

- تاریخچه:
  - آدرس‌دهی طبقه‌بندی شده (classful):
  - تعداد بیت‌های subnet ID بر اساس نوع کلاس مشخص می‌شد و نیاز به ماسک زیر شبکه نبود.
  - کلاس A: شبکه‌های خیلی بزرگ، ۸ بیت برای subnet ID و ۲۴ بیت برای host ID

  - کلاس B: شبکه‌های بزرگ، ۱۶ بیت برای subnet ID و ۱۶ بیت برای host ID



  - کلاس C: شبکه‌های بزرگ، ۲۴ بیت برای subnet ID و ۸ بیت برای host ID



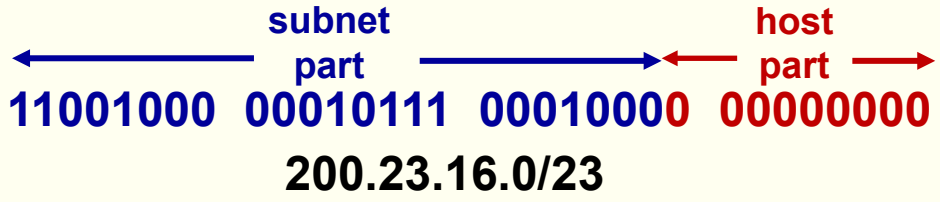
  - کنار گذاشته شدن آدرس‌دهی طبقه‌بندی شده: پر شدن فضای آدرس به دلیل هدر رفت فضای آدرس تخصیصی به یک شبکه
  - استفاده از روش آدرس‌دهی بدون طبقه: تخصیص آدرس بر اساس نیاز زیرشبکه و توانی از عدد ۲ (۱، ۲، ۴، ۸، ۱۶، ۳۲، ۶۴، ۱۲۸، ۲۵۶، ۵۱۲، ۱۰۲۴، ...)
  - (راه‌حل بلند مدت) افزایش تعداد بیت‌های فضای آدرس: IP ورژن ۶ (IPv6)

لایه شبکه – صفحه داده

پروتکل اینترنت (IP):

آدرس‌دهی IP: مسیریابی بین دامنه‌ای بدون طبقه‌بندی (CIDR – Classless Inter-Domain Routing):

- طول بخش subnet ID متغیر بر اساس نیاز شبکه به تعداد آدرس‌ها تعیین می‌شود.
- در جدول‌های جلورانی آدرس شبکه مقصد با دو عدد ۳۲ بیتی معرفی می‌شوند.
  - آدرس IP شبکه
  - ماسک زیر شبکه



- برای مقایسه تطابق آدرس ۳۲ بیتی مقصد (برداشته شده از سرآیند بسته دریافتی) ابتدا آدرس با ماسک شبکه and شده (حذف بیت‌های host ID) و سپس با آدرس شبکه مقصد مقایسه می‌شود.
- بدلیل وجود تجمیع آدرس‌ها (address aggregation) یا supernetting، در صورت مطابقت آدرس مقصد بسته با تعدادی از آدرس‌های شبکه مقصد در جدول جلورانی، بسته متعلق به شبکه‌ای است که بزرگترین تعداد بیت‌های net ID را دارد. در واقع جستجوی به روش تطابق طولانی‌ترین پیشوند (Longest prefix matching) انجام می‌شود (منظور از پیشوند همان net ID است).

لایه شبکه – صفحه داده

لایه شبکه اینترنت:

آدرس‌دهی IP: مسیریابی بین دامنه‌ای بدون طبقه‌بندی (CIDR – Classless Inter-Domain Routing):

- تطابق طولانی‌ترین پیشوند (Longest prefix matching)

Destination Address Range	Link interface
11001000 00010111 00010*** ********	0
11001000 00010111 00011000 ********	1
11001000 00010111 00011*** ********	2
otherwise	3

match!

match!

مثال: آدرس مقصد بسته دریافتی

11001000 00010111 00010110 10100001	which interface?
11001000 00010111 00011000 10101010	which interface?

لایه شبکه – صفحه داده

پروتکل پیکربندی پویای میزبان (DHCP – Dynamic Host Configuration Protocol):

دریافت (پیکربندی) آدرس IP:

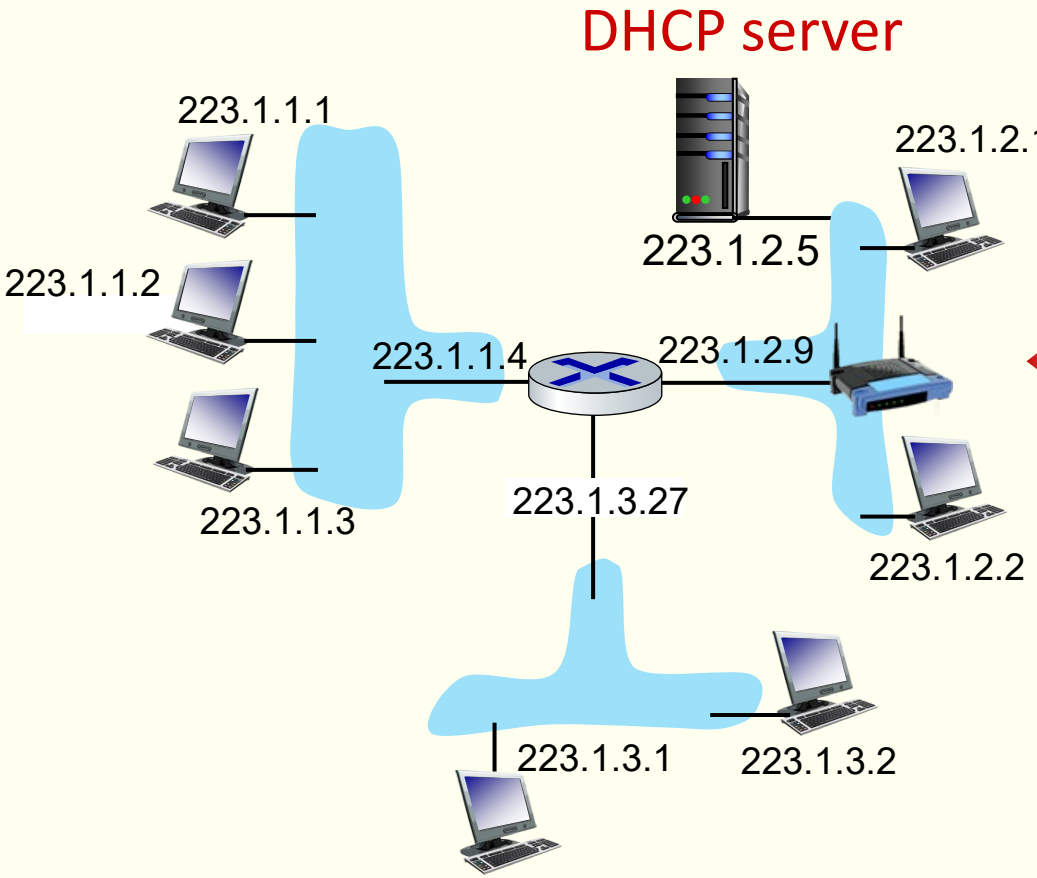
- هر واسط شبکه کامپیوتر میزبان باید یک آدرس IP داشته باشد.
- این آدرس یکی از آدرس‌های زیرشبکه‌ای است که کامپیوتر میزبان به آن متصل است و باید به واسط شبکه کامپیوتر میزبان تخصیص داده شده است.
- روش‌های انجام پیکربندی آدرس IP:
  - به صورت دستی توسط کاربر
    - بدلیل خطای انسانی امکان ورود اشتباه و ناسازگاری آدرس (address conflict) وجود دارد.
    - مدیریت استفاده مجدد از آدرس‌ها برای کامپیوترهای میزبان موقتی (کاربران موبایل) بسیار پیچیده است.
  - به صورت خودکار توسط سرویس‌دهنده DHCP (Dynamic Host Configuration Protocol)
    - انجام پیکربندی دقیق (حذف خطای انسانی در ورود آدرس تخصیصی)
    - تخصیص آدرس فقط به کامپیوترهای میزبان‌های فعال
    - تخصیص زمان‌دار (موقت) آدرس IP و امکان استفاده مجدد از آدرس‌ها آزاد شده
    - امکان تمدید زمان استفاده از آدرس تخصیصی

پروتکل پیکربندی پویای میزبان (DHCP – Dynamic Host Configuration Protocol):

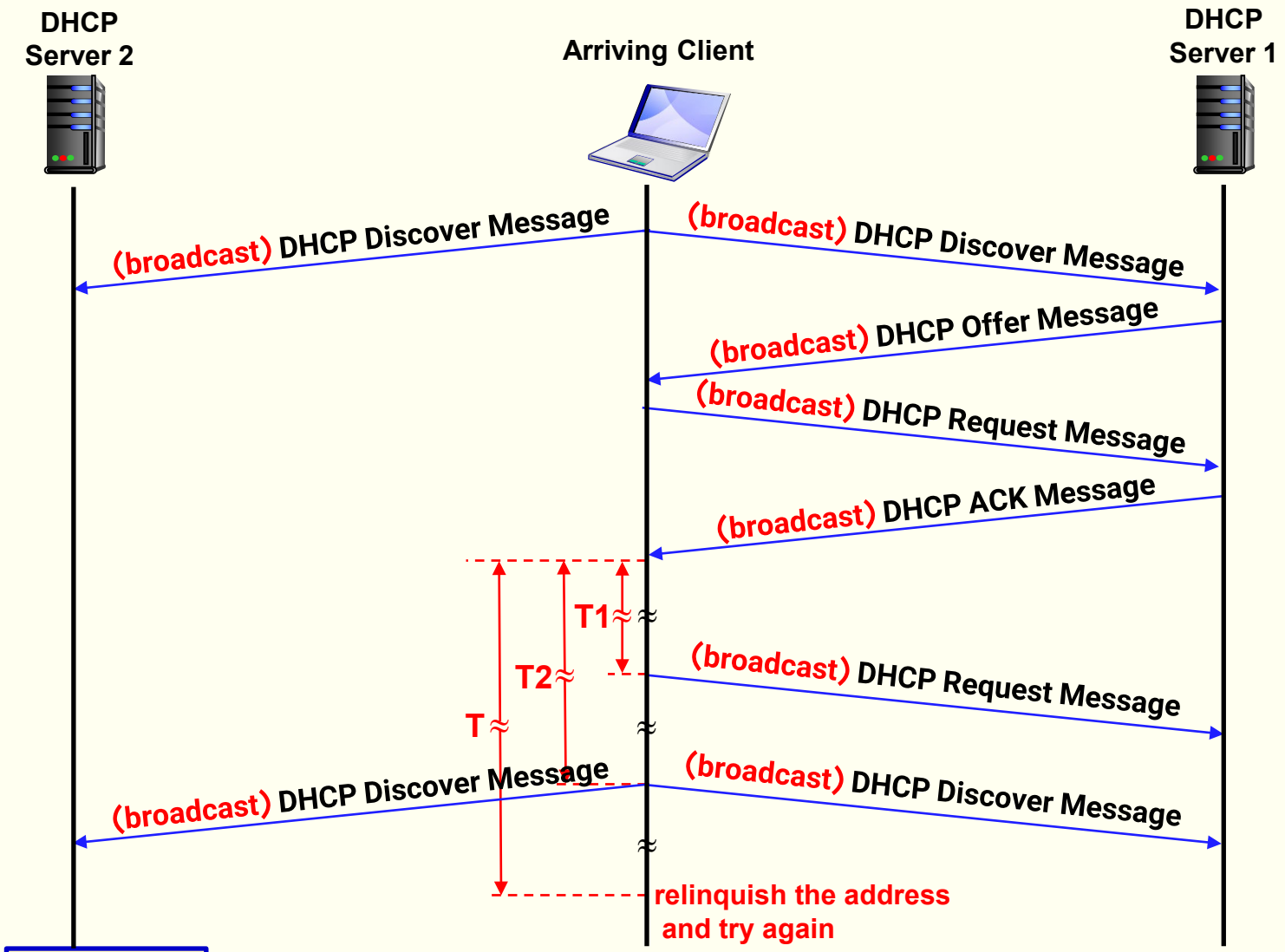
سناریو سرویس‌گیرنده-سرویس‌دهنده:

معمولاً سرویس‌دهنده DHCP درون مسیریاب قرار دارد و به تمام زیرشبکه‌هایی که به مسیریاب متصل هستند سرویس می‌دهد.

میزبان رسیده (سرویس‌گیرنده DHCP) نیاز به داشتن آدرس این شبکه دارد.



پروتکل پیکربندی پویای میزبان (DHCP – Dynamic Host Configuration Protocol):



نحوه پیکربندی کامپیوتر میزبان از طریق پروتکل DHCP:

۱) میزبان یک پیام کشف (پیداکردن) سرویس‌دهنده DHCP را زیرشبکه پخش همگانی (braodcast) می‌کند.

۲) سرویس‌دهنده‌های DHCP با ارسال پیام DHCP Offer به صورت پخش همگانی، آدرس IP ای پیشنهادی خود را برای میزبان اعلام می‌کنند.

۳) میزبان با دریافت پیام DHCP Offer، پیام DHCP Request را ارسال همگانی می‌کند.

۴) سرویس‌دهنده با دریافت پیام DHCP Request، با ارسال DHCP ACK، آدرس IP و سایر تنظیمات را به میزبان می‌دهد. در پیام تاییده زمان بهره‌برداری (T) از آدرس IP تخصیصی نیز به میزبانی داده می‌شود. میزبان همزمان ۳ زمانبند T1، T2 و T به ترتیب با زمان‌های 0.5T، 0.875T و T را روشن می‌کند. با منقضی شدن زمانبند T1 میزبان با ارسال پیام درخواست به سرویس‌دهنده DHCP سعی بر تمدید زمان بهره‌برداری از آدرس تخصیصی را دارد. اگر تا منقضی‌شدن زمانبند T2 میزبان، زمان بهره‌برداری تمدید نشد، میزبان سعی بر پیدا کردن و دریافت آدرس IP از یک سرویس‌دهنده DHCP دیگر دارد و اگر تا منقضی شده زمانبند T، میزبن تنواند آدرس IP خود را تمدید یا آدرس جدید دریافت کند، باید آدرس تخصیصی را آزاد کرده و مجاز با استفاده از آن نیست.

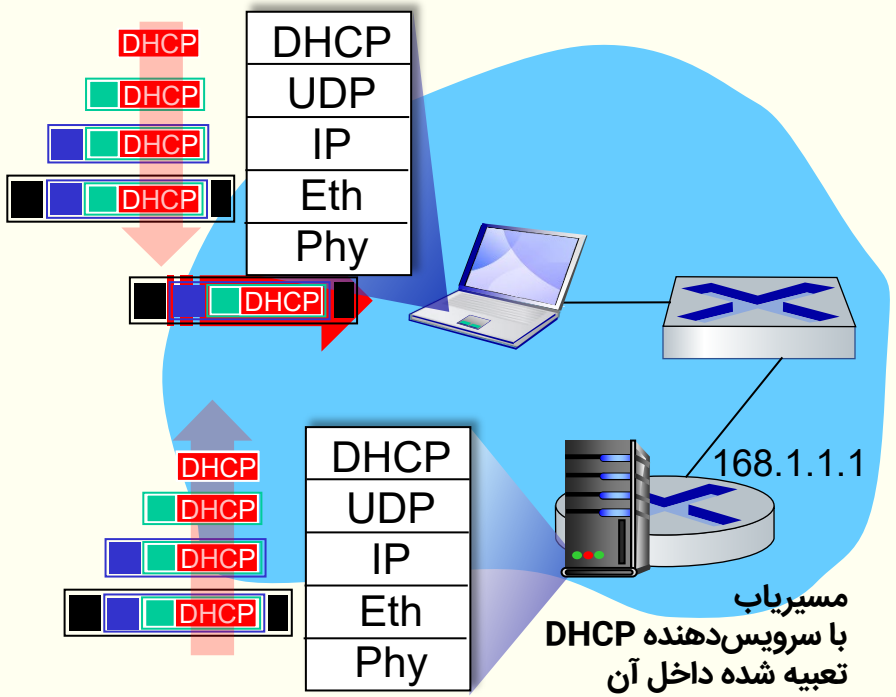
پروتکل پیکربندی پویای میزبان (DHCP – Dynamic Host Configuration Protocol):

انجام سایر پیکربندی‌های مورد نیاز برای استفاده از سرویس‌های اینترنت در زیر شبکه توسط سرویس‌دهنده DHCP

- آدرس مسیریاب گام اول (دروازه (gateway) شبکه)
- نام و آدرس IP سرویس‌دهنده DNS
- ماسک زیرشبکه (مشخص نمودن تعداد بیت‌های net ID)

پروتکل پیکربندی پویای میزبان (DHCP – Dynamic Host Configuration Protocol):

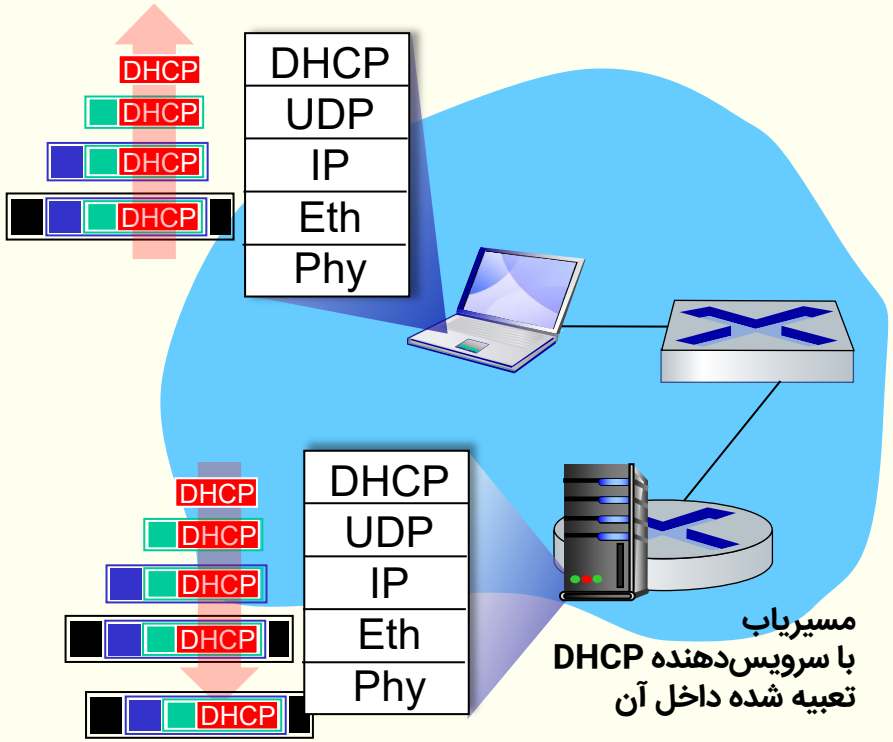
DHCP: مثال (سمت سرویس‌گیرنده)



- کامپیوتری که در حال اتصال به یک شبکه است، درخواستش برای دریافت آدرس IP و ماسک زیرشبکه، آدرس مسیریاب گام اول (دروازه) و آدرس سرویس‌دهنده DNS را به سرویس‌دهنده DHCP ارسال می‌کند.
- سرویس‌گیرنده مقدار شناسه تراکنش (transaction Identifier) در سرآیند پیام درخواست DHCP را برای تشخیص پاسخ تعیین می‌کند.
- پیام درخواست DHCP از طریق پروتکل UDP ارسال می‌شود (پورت UDP ۶۷ برای سرویس‌دهنده DHCP و پورت UDP ۶۸ برای سرویس‌گیرنده DHCP).
- سگمنت UDP از طریق بسته IP ارسال می‌شود. میزبان تا تخصیص آدرس IP از آدرس IP موقتی 0.0.0.0 استفاده می‌کند.
- فریم اترنت در زیرشبکه (شبکه LAN) ارسال همگانی می‌شود (آدرس مقصد: FFFFFFFFFFFF) و مسیریاب آن را دریافت می‌کند.

پروتکل پیکربندی پویای میزبان (DHCP – Dynamic Host Configuration Protocol):

DHCP: مثال (سمت سرویس‌دهنده)



- سرویس‌دهنده DHCP پیام تاییده CP شامل آدرس IP تخصیصی و ماسک زیرشبکه، آدرس مسیریاب گام اول (دروازه)، آدرس سرویس‌دهنده DNS و همچنین زمان بهره‌برداری (T) از آن را ارسال می‌کند.
- شناسه تراکنش (transaction Identifier) در سرآیند پیام تاییده همان شناسه تراکنش در پیام درخواست دریافتی است.
- پیام درخواست DHCP از طریق پروتکل UDP ارسال می‌شود (پورت UDP ۶۷ برای سرویس‌دهنده DHCP و پورت UDP ۶۸ برای سرویس‌گیرنده DHCP).
- سگمنت UDP از طریق بسته IP ارسال می‌شود.
- فریم اترنت در زیرشبکه (شبکه LAN) ارسال همگانی می‌شود (آدرس مقصد: FFFFFFFFFFFF) و کامپیوتر میزبان آن را دریافت می‌کند.

آدرس‌های اینترنت: نحوه تخصیص

هر تأمین‌کننده سرویس اینترنت (ISP) یک بلوک آدرس دارد.

ISP's block	11001000 00010111 00010000	00000000	200.23.16.0/20

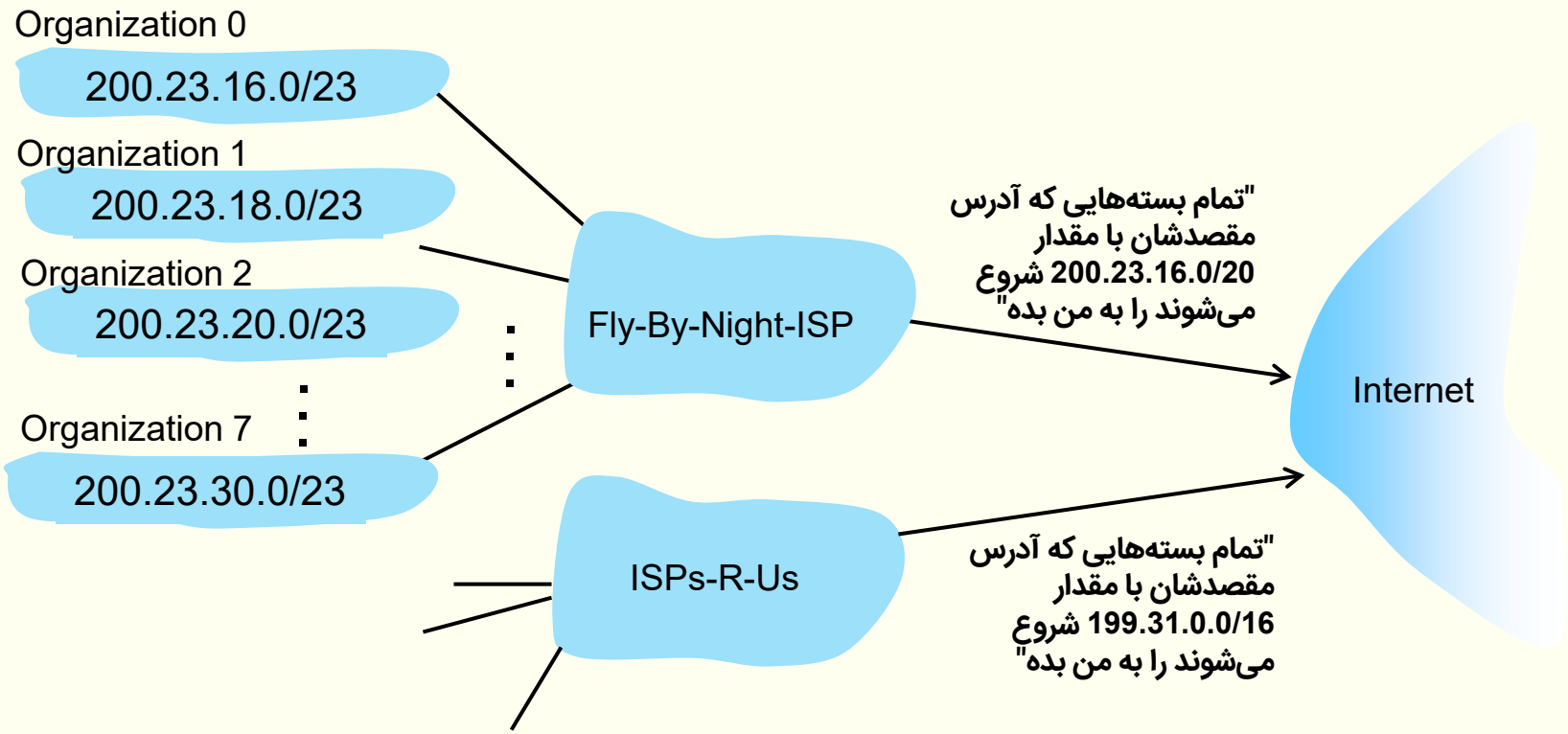
تأمین‌کننده سرویس اینترنت (ISP) بلوک آدرس خود را به تعدادی بلوک کوچک‌تر تقسیم می‌کند و هر بلوک را یک سازمان تخصیص می‌دهد.

Organization 0	11001000 00010111 00010000	00000000	200.23.16.0/23
Organization 1	11001000 00010111 00010010	00000000	200.23.18.0/23
Organization 2	11001000 00010111 00010100	00000000	200.23.20.0/23
...	.....	....	....
Organization 7	11001000 00010111 00011110	00000000	200.23.30.0/23

لایه شبکه – صفحه داده

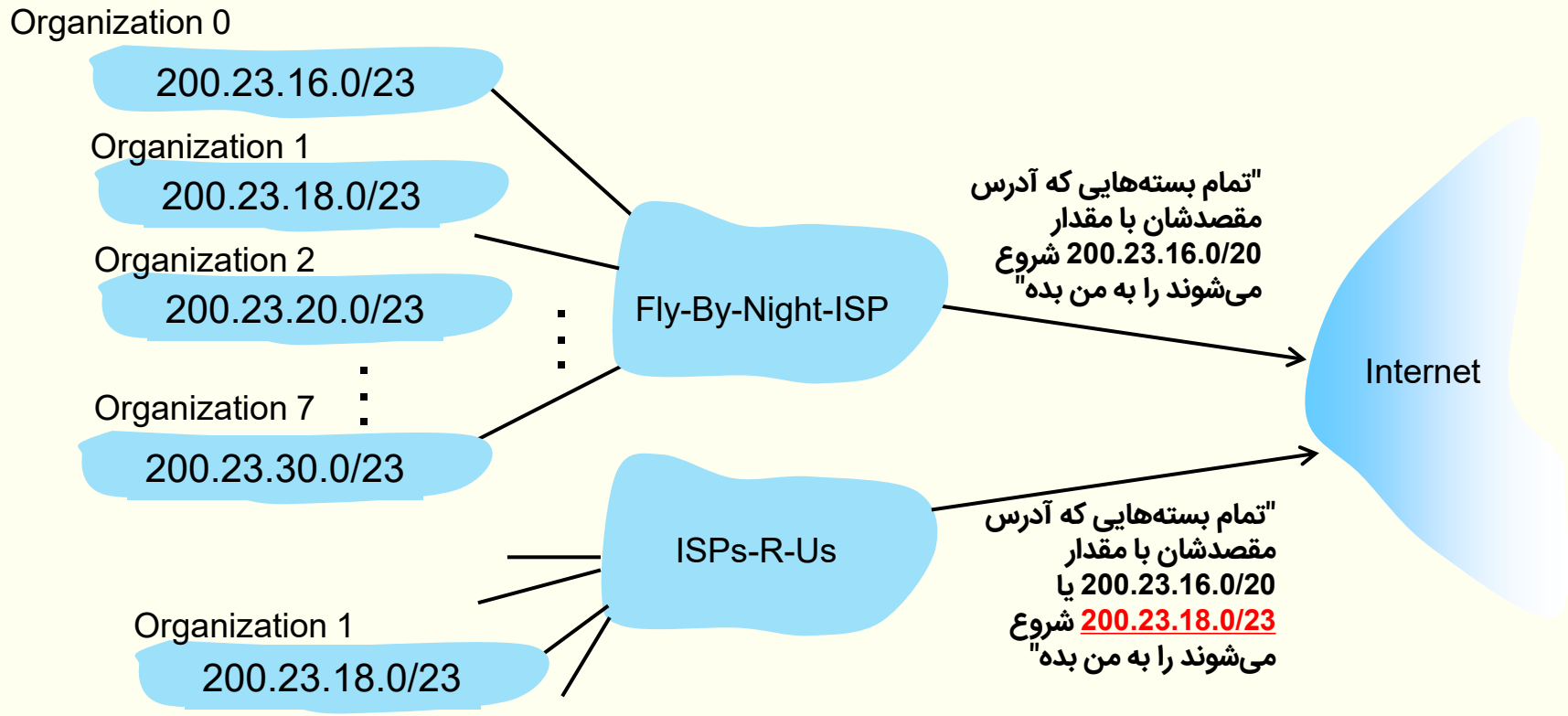
آدرس‌دهی سلسله‌مراتبی: تجمیع مسیر (route aggregation)

آدرس‌دهی سلسله‌مراتبی اجازه می‌دهد. اعلان اطلاعات مسیر به صورت کارآمد انجام شود.



آدرس‌دهی سلسله‌مراتبی: تجمیع مسیر (route aggregation)

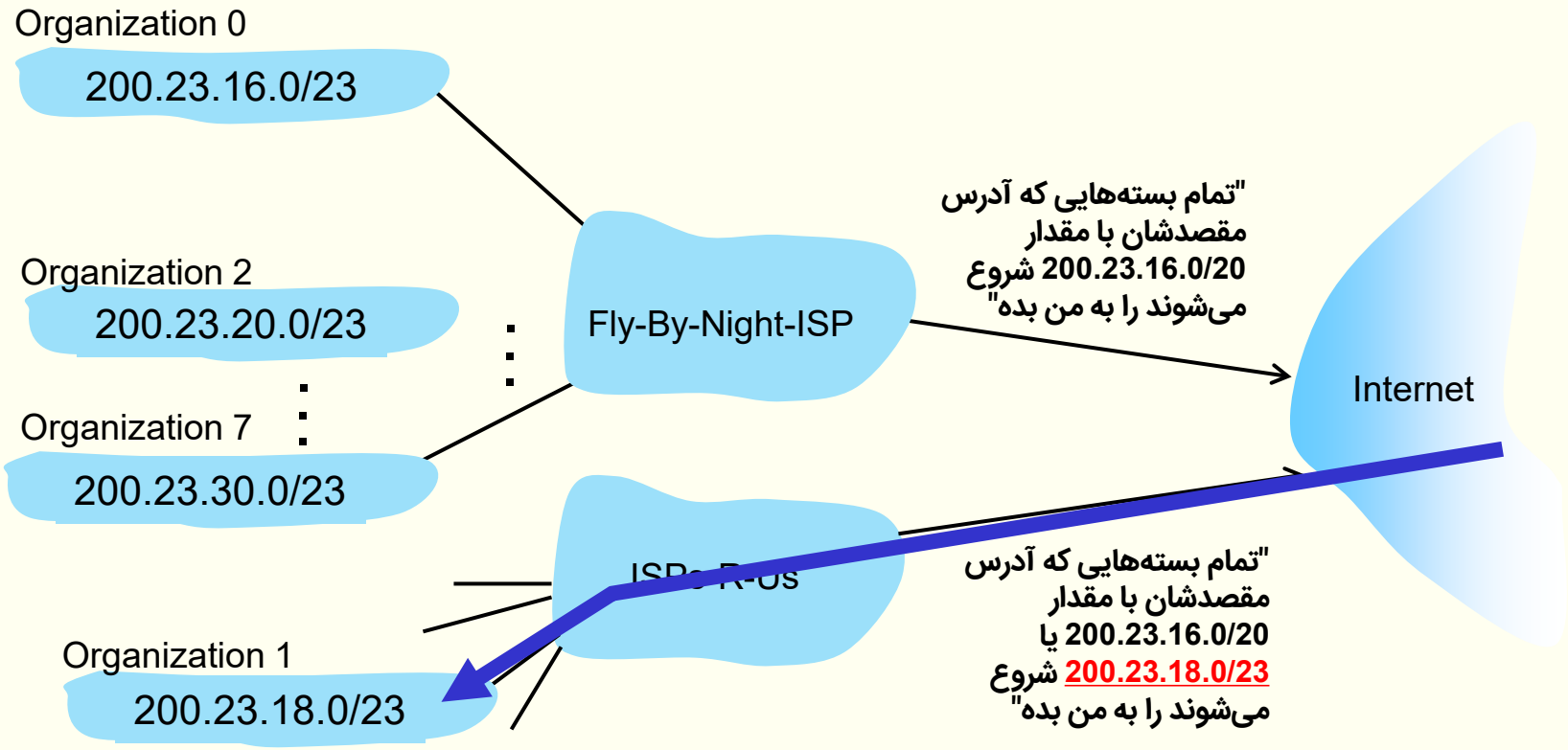
- سازمان ۱ از Fly-By-Night-ISP به ISPs-R-Us منتقل می‌شود.
- ISPs-R-Us علاوه بر اعلان‌های قبلی، حالا باید مسیر به سازمان ۱ را نیز اعلان کند.



لایه شبکه – صفحه داده

آدرس‌دهی سلسله‌مراتبی: تجمیع مسیر (route aggregation)

- سازمان ۱ از Fly-By-Night-ISP به ISPs-R-Us منتقل می‌شود.
- ISPs-R-Us علاوه بر اعلان‌های قبلی، حالا باید مسیر به سازمان ۱ را نیز اعلان کند.



لایه شبکه – صفحه داده

آدرس‌دهی اینترنت:

سازمان اینترنتی برای تخصیص نام‌ها و آدرس‌ها (ICANN: Internet Corporation for Names and Numbers)

www.icann.org

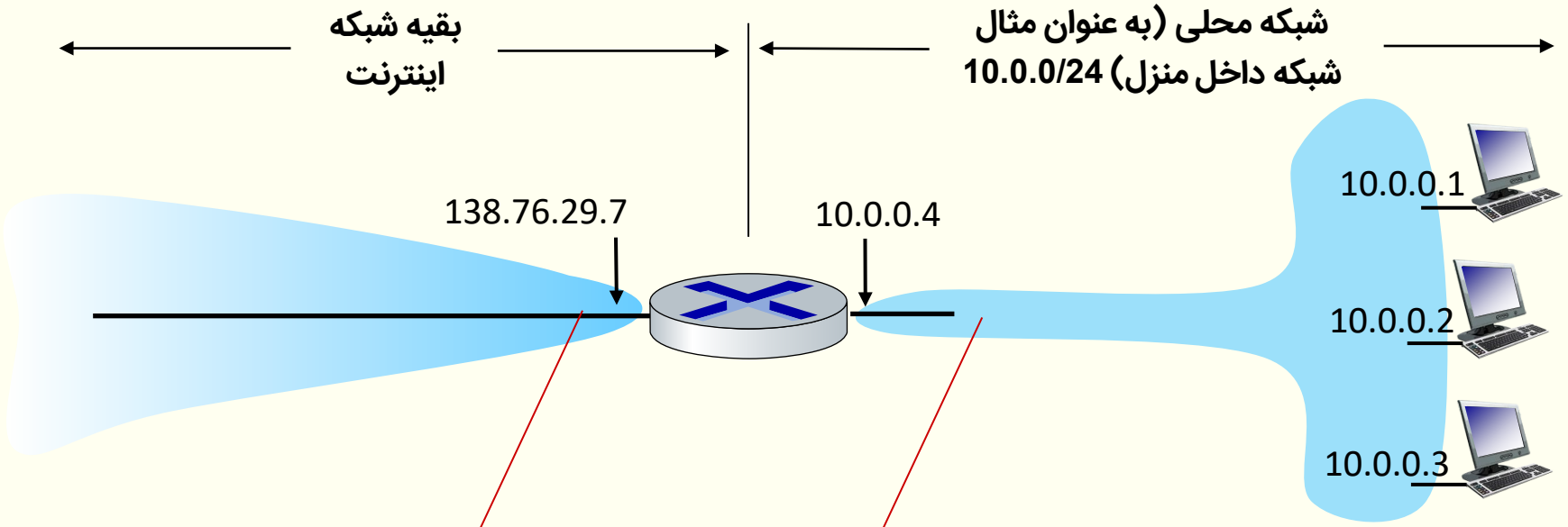
- تخصیص آدرس‌های IP از طریق ۵ دفتر ثبت‌نام منطقه‌ای (Regional Registries) (که آن‌ها نیز بلوک‌های آدرس را به دفترهای ثبت‌نام محلی تخصیص می‌دهند)
- مدیریت کردن منطقه‌ای DNSهای ریشه، شامل تفویض اختیار مدیریت دامنه‌های سطح بالا (TLD) نظیر .com، .edu و ...

سوال: آیا فضای آدرس ۳۲ بیتی برای شبکه اینترنت کافی است؟

- ICANN آخرین بلوک آدرس IPv4 را در سال ۲۰۱۱ به دفترهای ثبت‌نام منطقه‌ای تخصیص داد.
- NAT کمبود فضای آدرس IPv4 را جبران کرده است.
- در پروتکل IPv6 فضای آدرس ۱۲۸ بیتی شده است.

تبدیل آدرس شبکه (NAT – Network Address Translation)

NAT: تمام وسایل (کامپیوترها، مسیریاب‌ها و ...) داخل یک شبکه محلی می‌تواند از طریق فقط یک آدرس IPv4 به شبکه اینترنت متصل شوند.



بسته‌های با آدرس مبدأ یا آدرس مقصد در این شبکه آدرس‌هایی از محدود 10.0.0/24 برای آدرس مبدأ یا آدرس مقصد دارند.

تمام بسته‌هایی که از این شبکه محلی خارج می‌شوند آدرس مبدأ یکسان تبدیل شده توسط NAT را دارند: آدرس ۱۳۸.۷۶.۲۹.۷ اما با شماره پورت‌های مبدأ مختلف.

تبدیل آدرس شبکه (NAT – Network Address Translation)

- تمام دستگاه‌ها در یک شبکه محلی آدرس‌های ۳۲ بیتی از فضای آدرس‌های "خصوصی" (آدرس‌های با پیشوند 10.0.0.0/8، 172.16.0.0/12 و 192.168.0.0/16) را دارند که فقط قابل استفاده در شبکه محلی است.

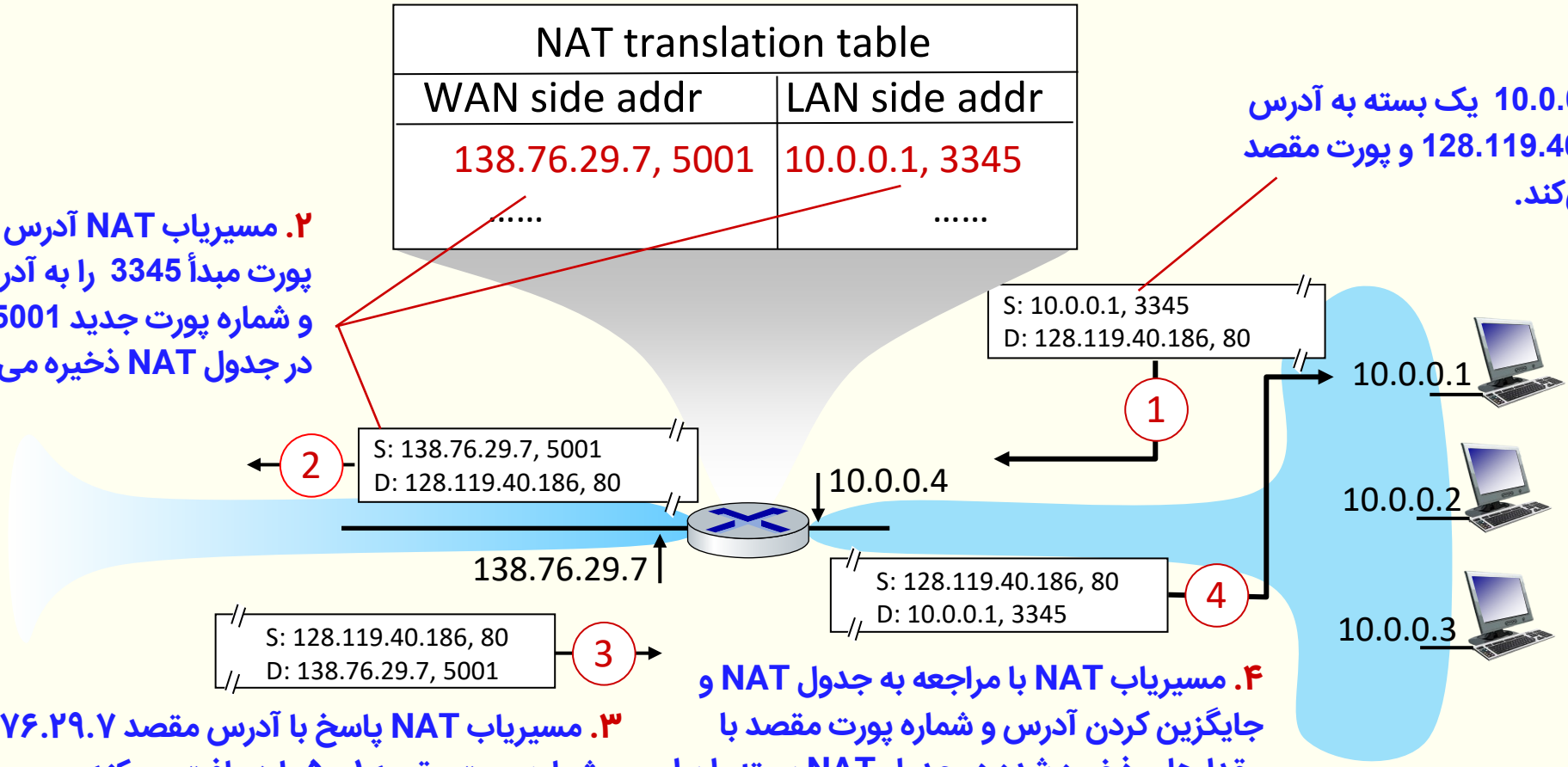
- **مزیت‌ها:**
  - فقط لازم است برای تمام دستگاه‌ها یک آدرس IP اختصاص داده شود.
  - بدون اطلاع‌رسانی به بقیه شبکه اینترنت، می‌توان آدرس IP کامپیوترهای میزبان را تغییر داد.
  - بدون انجام تغییر در آدرس‌های IP دستگاه‌های داخل شبکه، می‌توان ISP را تغییر داد.
  - دستگاه‌های داخل شبکه محلی مستقیماً توسط بقیه شبکه اینترنت قابل مشاهده و دسترسی نیستند (افزایش امنیت)

تبدیل آدرس شبکه (NAT – Network Address Translation)

نحوه پیاده‌سازی: مسیریاب NAT می‌بایست به صورت شفاف (بدون آنکه دستگاه‌ها متوجه شوند) تبدیل آدرس را انجام دهد.

- بسته‌های خارج‌شده: جایگزین کردن (آدرس IP و شماره پورت مبدأ) هر بسته خارج‌شده با (آدرس NAT IP و شماره پورت جدید)
- سرویس‌دهنده یا سرویس‌گیرنده خارج از شبکه محلی با آدرس NAT IP و شماره پورت جدید به عنوان آدرس مقصد پاسخ می‌دهد.
- نگهداری تبدیل (آدرس IP و شماره پورت مبدأ) به (آدرس NAT IP و شماره پورت جدید) در جدول تبدیل NAT (NAT Translation Table)
- بسته‌های واردشده: جایگزین کردن (آدرس NAT IP و شماره پورت جدید) در فیلدهای مقصد هر بسته وارد شده با (آدرس IP و شماره پورت مبدأ) ذخیره شده در جدول NAT.

تبدیل آدرس شبکه (NAT – Network Address Translation)



۱. میزبان 10.0.0.1 یک بسته به آدرس مقصد 128.119.40.186 و پورت مقصد 80 ارسال می‌کند.

۲. مسیریاب NAT آدرس مبدأ 10.0.0.1 و شماره پورت مبدأ 3345 را به آدرس NAT 138.76.29.7 و شماره پورت جدید 5001 جایگزین کرده و آن را در جدول NAT ذخیره می‌کند.

۳. مسیریاب NAT پاسخ با آدرس مقصد ۱۳۸.۷۶.۲۹.۷ و شماره پورت مقصد ۵۰۰۱ را دریافت می‌کند.

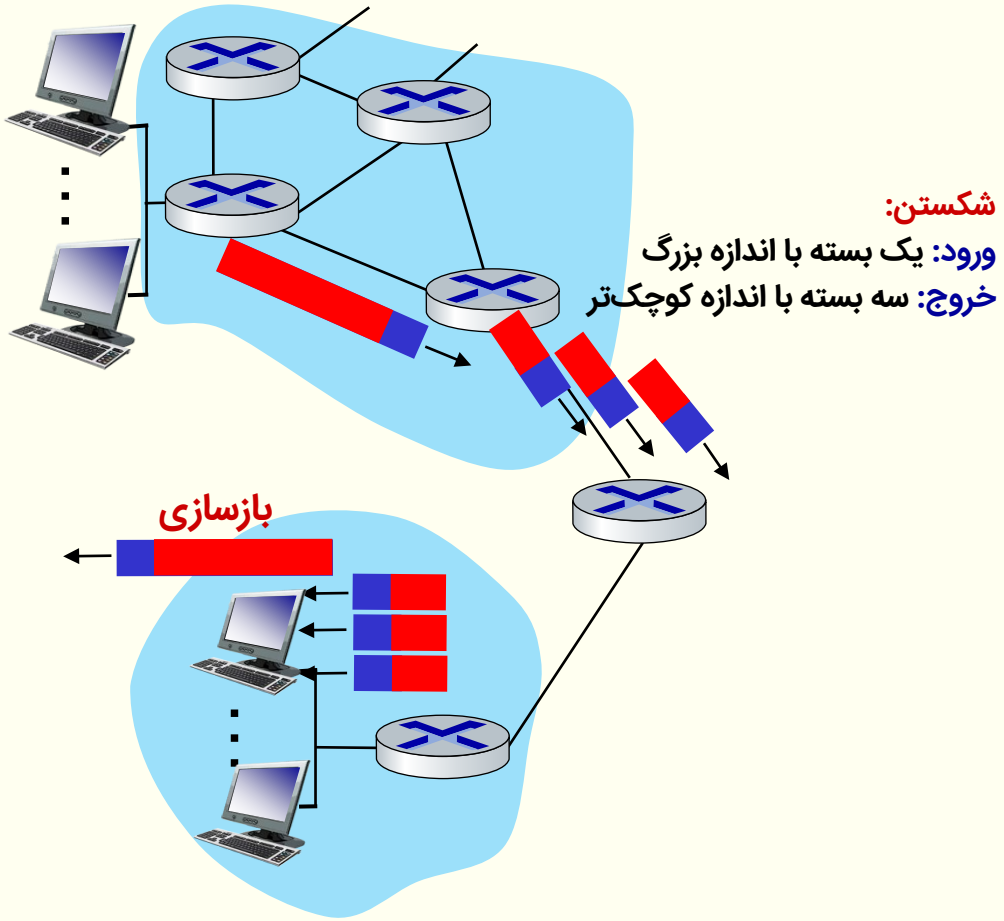
۴. مسیریاب NAT با مراجعه به جدول NAT و جایگزین کردن آدرس و شماره پورت مقصد با مقدارهای ذخیره شده در جدول NAT بسته را برای میزبان 10.0.0.1 ارسال می‌کند.

تبدیل آدرس شبکه (NAT – Network Address Translation)

- استفاده از NAT بحث برانگیز است:
  - نقض مفهوم مدل لایه‌ای: مسیریاب باید تا لایه ۳ پردازش کند (استفاده از فیلد شماره پورت از لایه ۴).
  - مسئله کمبود آدرس باید با پیاده‌سازی IPv6 حل شود.
  - بحث در مورد نقض عملیات انتها به انتها (شماره پورت توسط دستگاه‌های لایه شبکه تغییر می‌کند)
  - پیمایش NAT: نحوه متصل شدن سرویس‌گیرنده‌ها به سرویس‌دهنده‌های پشت NAT
- اما NAT همچنان استفاده می‌شود:
  - به خصوص در شبکه‌های داخل منزل، شبکه‌های سازمانی و دانشگاه‌ها و شبکه‌های داده سلولی 4G و 5G

خُردسازی و بازسازی بسته‌های IP (IP fragmentation/reassembly)

- هر واسط شبکه یک واحد انتقال حداکثری (MTU – Maximum Transfer Unit) دارد:
  - واحد انتقال حداکثری (MTU) وابسته به نوع فناوری واسط شبکه است و هر فناوری یک مقدار MTU دارد. به عنوان مثال MTU برای شبکه‌های اترنت ۱۵۰۰ بایت است.
- بسته‌های با اندازه بزرگتر از MTU باید به بسته‌های کوچک‌تر خرد شده و در گره میزبان نهایی بازسازی می‌شوند.
- خُردسازی (fragmentation) ممکن است در گره مبدأ و گره‌های میانی انجام شود.
- بازسازی (reassembly) فقط در گره مقصد انجام می‌شود.
- در سرآیند بسته‌های IP سه فیلد برای انجام خُردسازی و بازسازی وجود دارد:
  - identification
  - flags شامل دو پرچم MF و DF
  - fragment offset



خُردسازی و بازسازی بسته‌های IP (IP fragmentation/reassembly)

فیلدهای سرآیند برای انجام خردسازی و بازسازی بسته‌های IP (IP fragmentation/reassembly)

- **شناسه (identification):**
  - یک عدد ۱۶ بیتی است که گره مبدأ به عنوان شناسه به هر بسته اختصاص می‌دهد.
  - تمام بسته‌های خُرد شناسه بسته اصلی را دارند.
- **بیت‌های پرچم (flags):**
  - MF: بیت پرچم MF (more fragmentation) در سرآیند هر بسته خرد مشخص می‌کند که بسته خرد بعدی وجود دارد یا خیر.
    - $MF = 1$: بسته خرد اول یا میانی
    - $MF = 0$: بسته خرد آخر
  - DF: بیت پرچم DF (don't fragment) مشخص می‌کند که گره میانی مجاز به خردسازی بسته هست یا خیر.
    - اگر بیت DF یک بسته دریافتی توسط یک مسیریاب یک باشد ($DF = 1$) و جلورانی آن بسته به گره بعدی نیاز به خردسازی بسته داشته باشد، آن بسته حذف شده و این خطا از طریق پیام گزارش خطای ICMP به گره مبدأ اعلام می‌گردد.
- **مکان خردسازی‌شده (fragmentation offset):**
  - اگر اندازه بسته دریافتی از MTU واسط شبکه مسیریاب بعدی بزرگ‌تر باشد، فیلد داده بسته اصلی به تعدادی قطعه خرد می‌شود.
  - هر قطعه خرد تبدیل به یک بسته خرد می‌شود.
  - fragmentation offset مکان قطعه در داده بسته اصلی را مشخص می‌کند.
  - از آنجایی که اندازه یک بسته IP حداکثر ۶۴ کیلوبایت است، بنابراین fragmentation offset یک عدد ۱۶ بیتی خواهد بود.
  - فیلد fragmentation offset در سرآیند بسته IP یک فیلد ۱۳ بیتی است. بنابراین داده بسته اصلی به قطعاتی با اندازه مضرب ۸ خرد می‌شود تا همواره fragmentation offset یک عدد مضرب ۸ باشد (۳ بیت کم ارزش آن صفر است) و مقدار تقسیم بر ۸ fragmentation offset در فیلد fragmentation offset بسته خرد قرار می‌گیرد.

خُردسازی و بازسازی بسته‌های IP (IP fragmentation/reassembly)

نحوه انجام خردسازی و بازسازی بسته‌های IP (IP fragmentation/reassembly)

۱. بدست آوردن بزرگ‌ترین عدد مضرب ۸ کوچک‌تر از $(MTU - 20)$

۲.خردکردن فیلد داده بسته اصلی به قطعه‌های با اندازه عدد بدست آمده در بند ۱ (قطعه آخر ممکن است اندازه کوچک‌تر از بقیه داشته باشد).

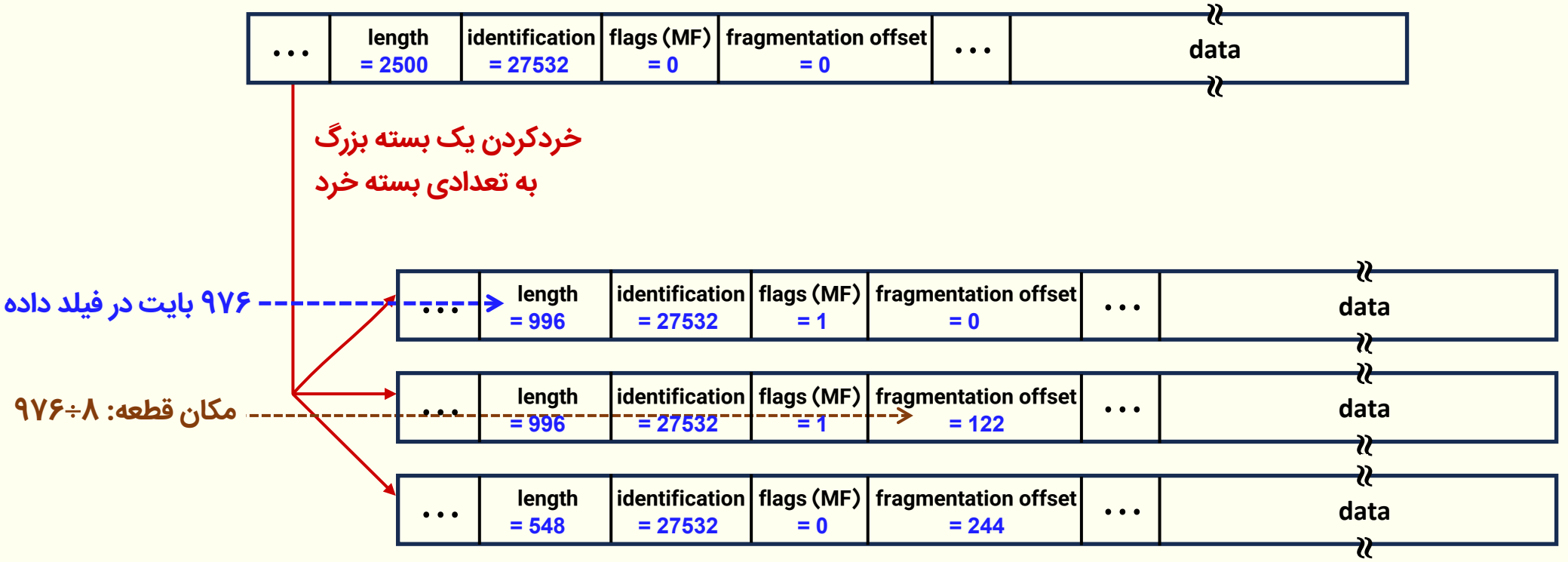
۳.هر قطعه خرد با اضافه شدن سرآیند یک بسته خرد تبدیل شده و در واسط شبکه مسیریاب بعدی ارسال (جلورانی) می‌شود:

- فیلد شناسه بسته‌های خرد همان مقدار شناسه بسته اصلی را دراد.
- بیت پرچم MF برای بسته‌های خرد اول و میانی مقدار یک $(MF = 1)$ و برای بسته خرد آخر مقدار صفر $(MF = 0)$ دارد.
- فیلد fragmentation offset بسته‌های خرد مقدار تقسیم بر ۸ offset واقعی را دارد.
- فیلد طول کل (total length) برابر است با اندازه (قطعه) داده بعلاوه اندازه سرآیند
- بقیه فیلدهای سرآیند بسته‌های خرد مقدار سرآیند بسته اصلی را دارند.
- مقدار فیلد بیت‌های چک‌کننده جمع (checksum) مجدداً محاسبه می‌شود.

خُردسازی و بازسازی بسته‌های IP (IP fragmentation/reassembly)

مثال:

- اندازه بسته دریافتی ۲۵۰۰ بایت
- واحد انتقال حداکثر واسط شبکه گره بعدی $MTU = 1000$ bytes
- بزرگ‌ترین عدد مضرب ۸ کوچک‌تر از ۹۸۰ برابر است با : ۹۷۶



پروتکل IP نسخه ۶ (IPv6):

انگیزه‌های تعریف پروتکل IPv6:

- انگیزه اولیه:
  - محدودیت فضای آدرس ۳۲ بیتی در پروتکل IPv4
- انگیزه‌های دیگر:
  - بهبود کارآیی (performance) پروتکل IPv4 با ساده‌سازی سرآیند پروتکل IPv6 (امکان افزایش سرعت سوییچینگ با ثابت‌سازی اندازه فیلدهای سرآیند و حذف بعضی از فیلدهای غیرضروری)
  - افزودن ویژگی‌های جدید به منظور بهبود عملکرد
  - جایگزینی یا تغییر نام بعضی از فیلدهای سرآیند به منظور بیان عملکرد واقعی آن‌ها

پروتکل IP نسخه ۶ (IPv6):

ویژگی‌های پروتکل IPv6:

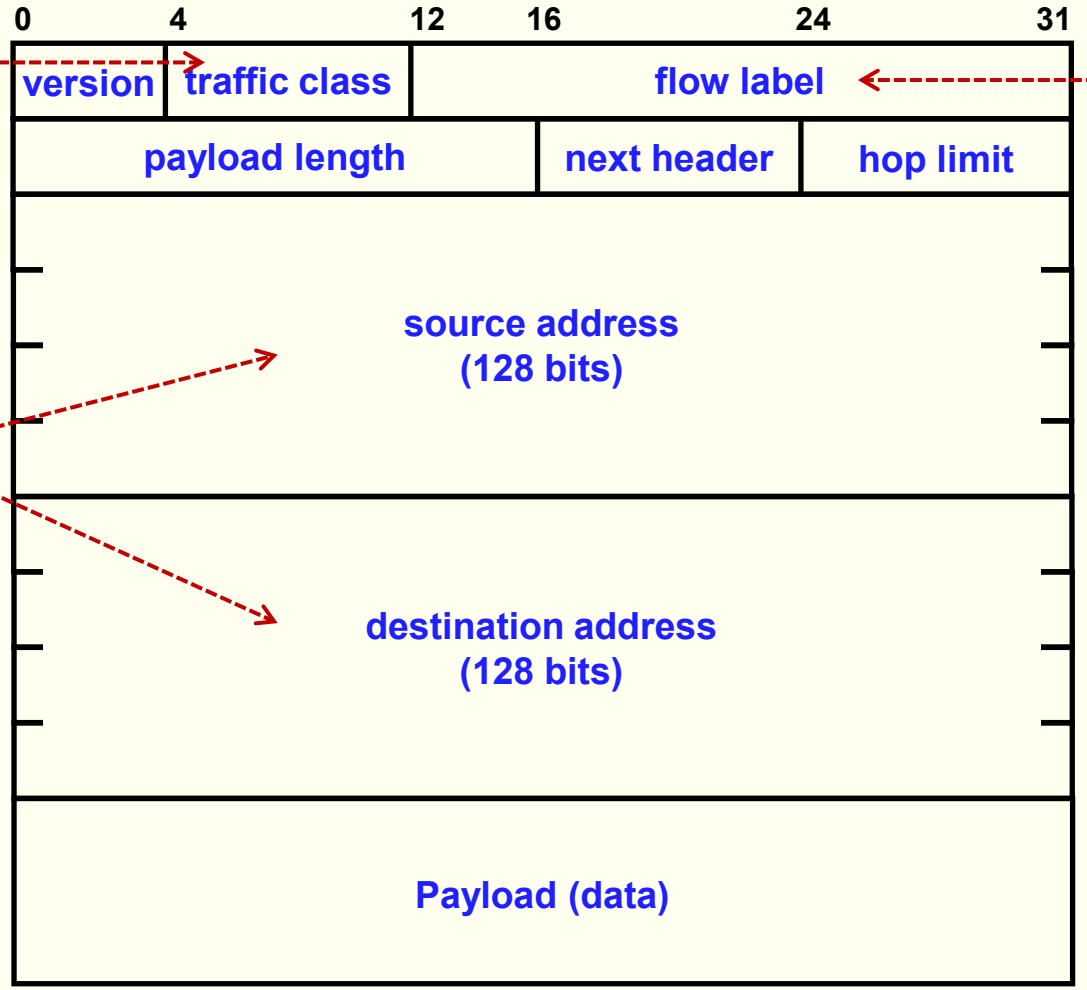
- **افزایش فضای آدرس:**
  - فیلد آدرس از ۳۲ بیت در پروتکل IPv4 به ۱۲۸ بیت در پروتکل IPv6 افزایش یافته است.
- **بهبود عملکرد:**
  - اضافه کردن فیلد flow label (برای شناسایی آسان بسته‌های متعلق به یک جریان ترافیکی و ارائه سرویس مشابه با بسته‌های متعلق به یک جریان و ارائه سرویس متمایز به جریان‌های مختلف با هدف بهبود کیفیت سرویس‌دهی و افزایش گذردهی)
  - حذف محدودیت استفاده از optionها
  - افزودن مکانیزم‌های امنیتی
- **ساده‌سازی سرآیند:**
  - ثابت بودن اندازه سرآیند
  - حذف فیلدهای identification، flags، fragmentation offset و checksum
  - خُردسازی بسته فقط در مبدأ انجام می‌شود.
- **جایگزینی فیلدها (در پروتکل IPv6 در مقایسه با پروتکل IPv4):**
  - جایگزینی فیلد datagram length با payload length
  - جایگزینی فیلد protocol با next header
  - جایگزینی فیلد type of service با traffic class
  - جایگزینی فیلد TTL با hop limit

پروتکل IP نسخه ۶ (IPv6):

فرمت بسته‌های پروتکل IPv6:

کلاس ترافیکی:
مشخص کننده الویت بسته‌ها در جریان ترافیکی

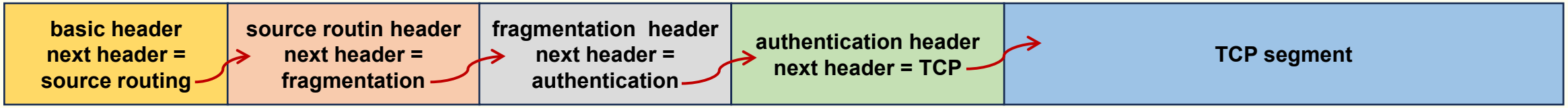
برچسب جریان:
مشخص کننده بسته متعلق به یک جریان (مفهوم جریان به صورت دقیق تعریف نشده است)



فیلدهای آدرس ۱۲۸ بیتی در پروتکل IPv6

پروتکل IP نسخه ۶ (IPv6):

توسعه سرآیندهای اختیاری (options) به صورت زنجیره پشت‌سرهم و بدون محدودیت:

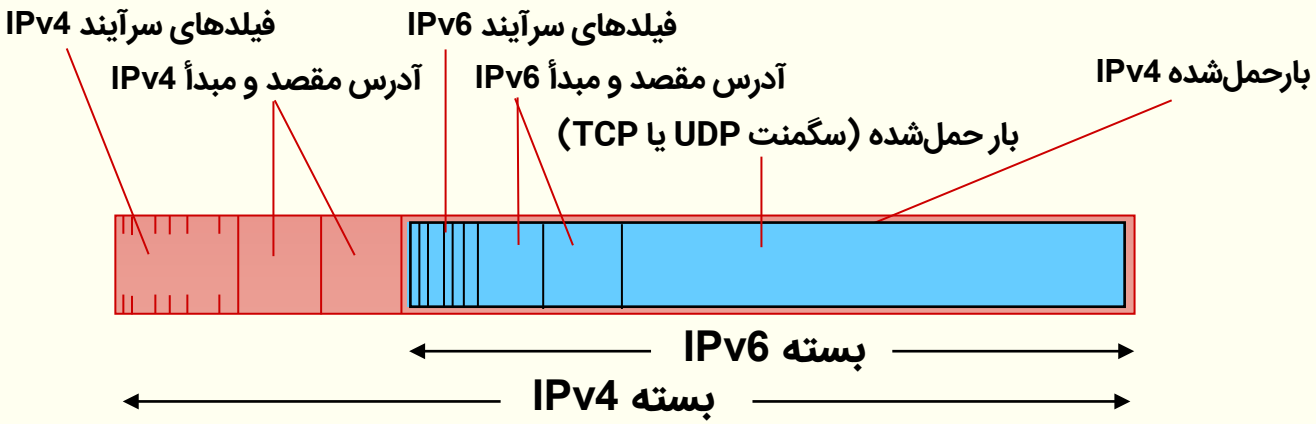


پروتکل IP نسخه ۶ (IPv6):

گذر از IPv4 به IPv6:

- ارتقاء تمام مسیریاب‌ها به صورت همزمان از پروتکل IPv4 به IPv6 امکان‌پذیر نیست.
  - هنوز روزی به عنوان مهلت نهایی تعیین نشده است.
  - چگونه شبکه می‌تواند به صورت ترکیبی از پروتکل‌های IPv4 و IPv6 کار کند.

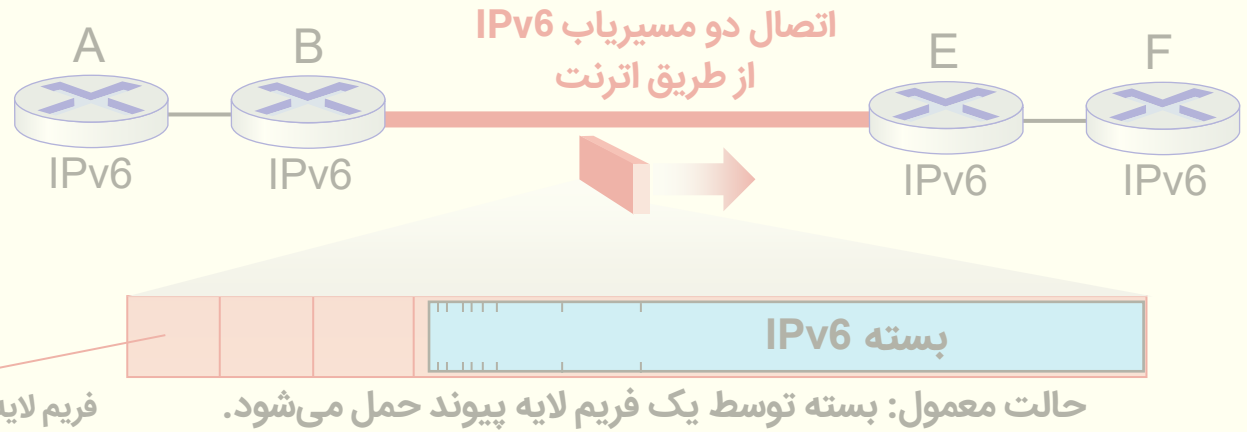
- تونل‌سازی (tunneling):
  - بسته‌های IPv6 به عنوان داده (بارحمل‌شده) توسط بسته‌های IPv4 حمل شده و از شبکه عبور می‌کنند (بسته‌ای داخل یک بسته).
  - تونل‌سازی در زمینه‌های دیگر نیز استفاده می‌شوند (VPN، 4G، 5G و ...)



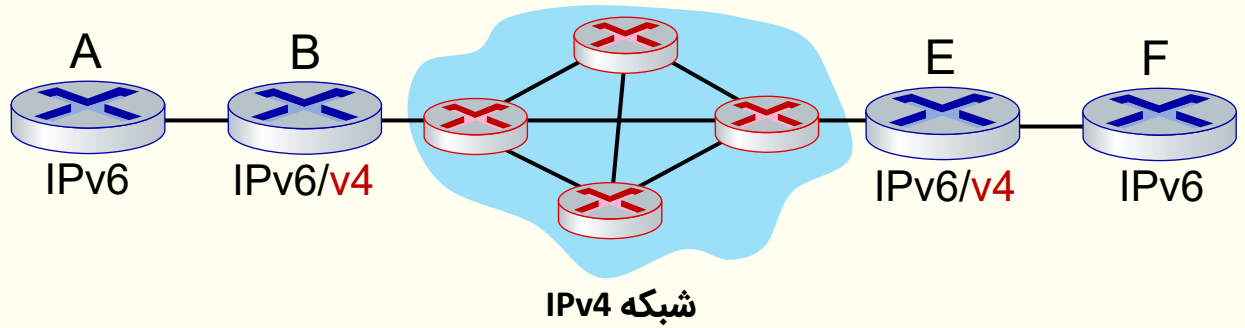
پروتکل IP نسخه ۶ (IPv6):

تونل‌سازی و کپسوله‌کردن:

اتصال دو مسیریاب IPv6 از طریق شبکه اترنت (حالت معمول)



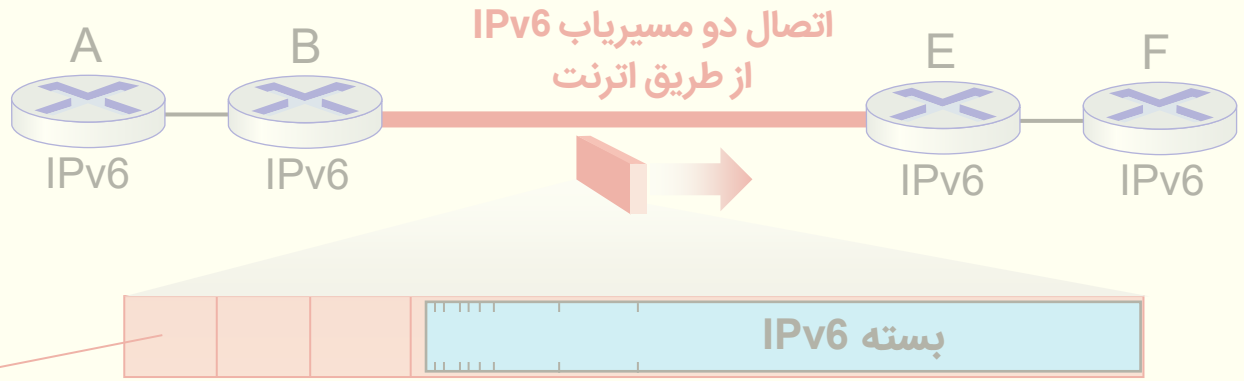
اتصال دو مسیریاب IPv6 از طریق شبکه IPv4



پروتکل IP نسخه ۶ (IPv6):

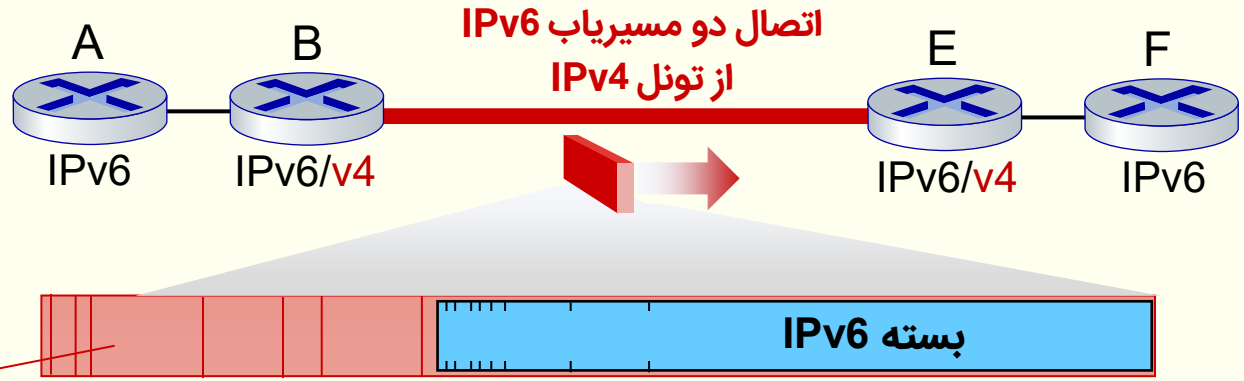
تونل‌سازی و کپسوله‌کردن:

اتصال دو مسیریاب IPv6 از طریق شبکه اترنت (حالت معمول)



حالت معمول: بسته توسط یک فریم لایه پیوند حمل می‌شود.

اتصال دو مسیریاب IPv6 از طریق شبکه IPv4

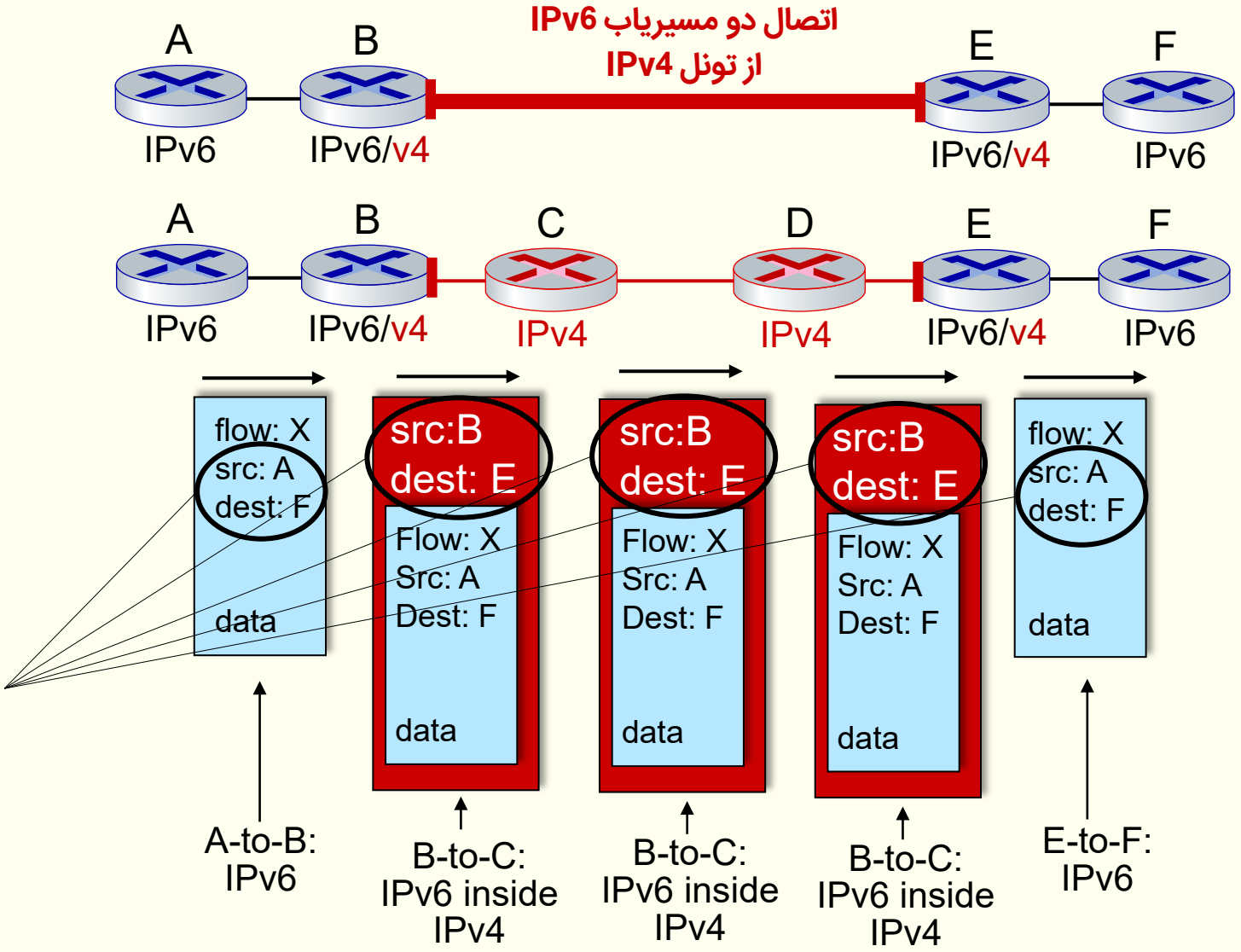


تونل‌سازی: بسته IPv6 به عنوان داده (بارحمل‌شده) در بسته IPv4 قرار می‌کیرد.

لایه شبکه – صفحه داده

پروتکل IP نسخه ۶ (IPv6):

تونل‌سازی:

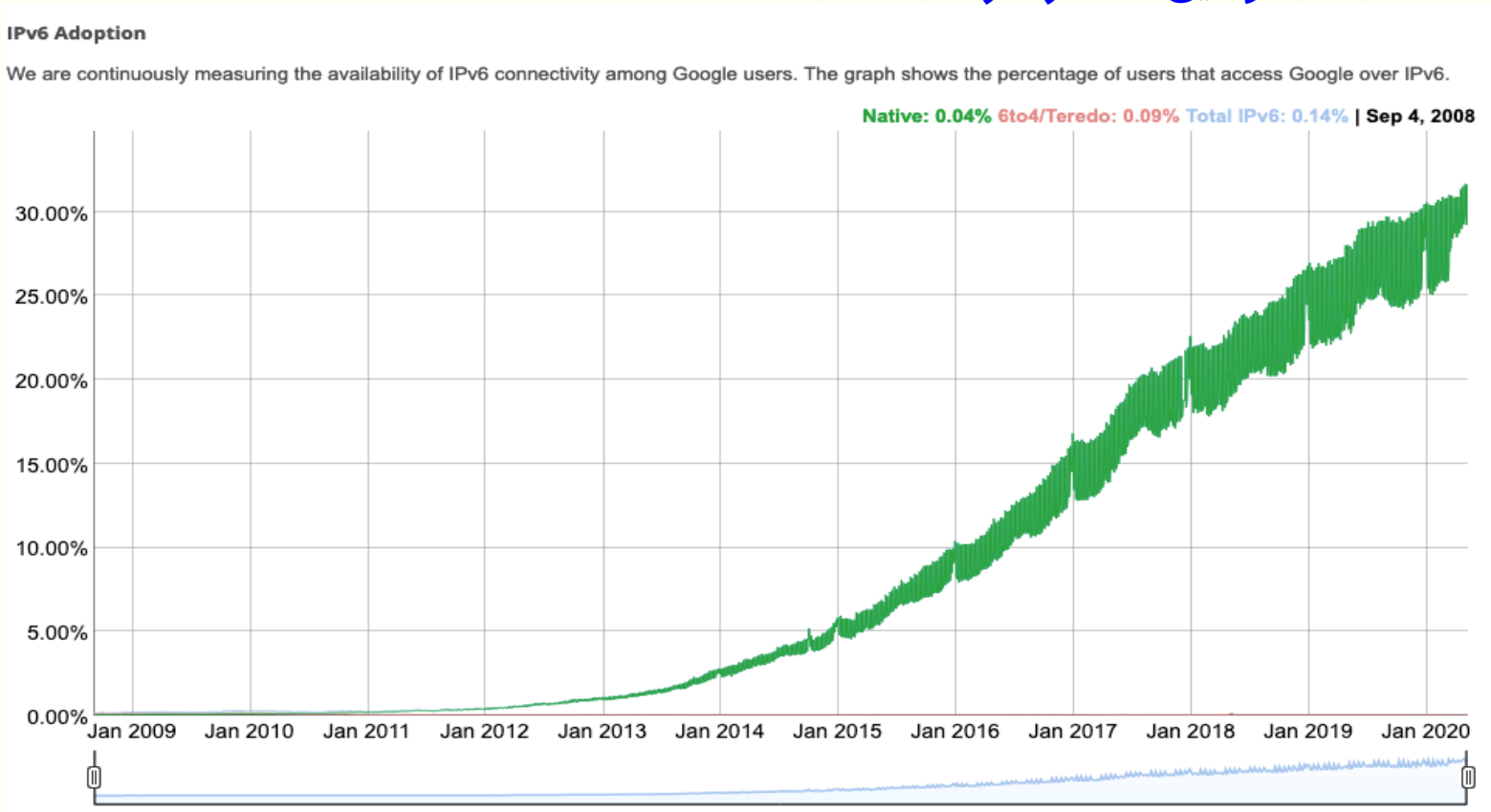


لایه شبکه – صفحه داده

پروتکل IP نسخه ۶ (IPv6):

میزان پذیرش IPv۶:

- حدود ۳۰ درصد سرویس‌گیرنده‌ها از طریق سرویس‌های IPv6 به شبکه اینترنت دسترسی دارند. (گوگل[1])
- یک سوم تمام دامنه‌های دولت ایالات متحده (US) توانایی IPv6 را دارند (NIST)



[1] https://www.google.com/intl/en/ipv6/statistics.html

پروتکل IP نسخه ۶ (IPv6):

میزان پذیرش IPv۶:

- حدود ۳۰ درصد سرویس‌گیرنده‌ها از طریق سرویس‌های IPv6 به شبکه اینترنت دسترسی دارند. (گوگل[1])
- یک سوم تمام دامنه‌های دولت ایالات متحده (US) توانایی IPv6 را دارند (NIST).
- زمان استقرار بسیار طولانی:
  - ۳۰ سال گذشته و هنوز ادامه دارد!
  - تغییرات برنامه‌های کاربردی در ۳۰ سال گذشته:
    - کنفرانس‌ها و ارائه‌های از راه‌دور
    - بازی‌ها
    - شبکه‌های اجتماعی
    - پخش (جریان‌سازی) رسانه (صوت و ویدیو)
    - واقعیت مجازی
    - ...
- چرا استقرار IPv6 به این میزان طولانی‌شده و هنوز هم انجام نشده است؟