امنیت
مدل اُ-اس-آی

محسن هوشمند
دانشکده تکنولوژی اطلاعات و علم رایانه
دانشگاه تحصیلات تکمیلی علوم پایه زنجان

مدل ا-اس-آی ایزو

ISO ایزو سازمانی است با نام سازمان استانده‌های بین‌الملل

OSI ارتباط درونی سیستم باز

مدل

کاربرد

نمایش

جلسه

انتقال

شبکه

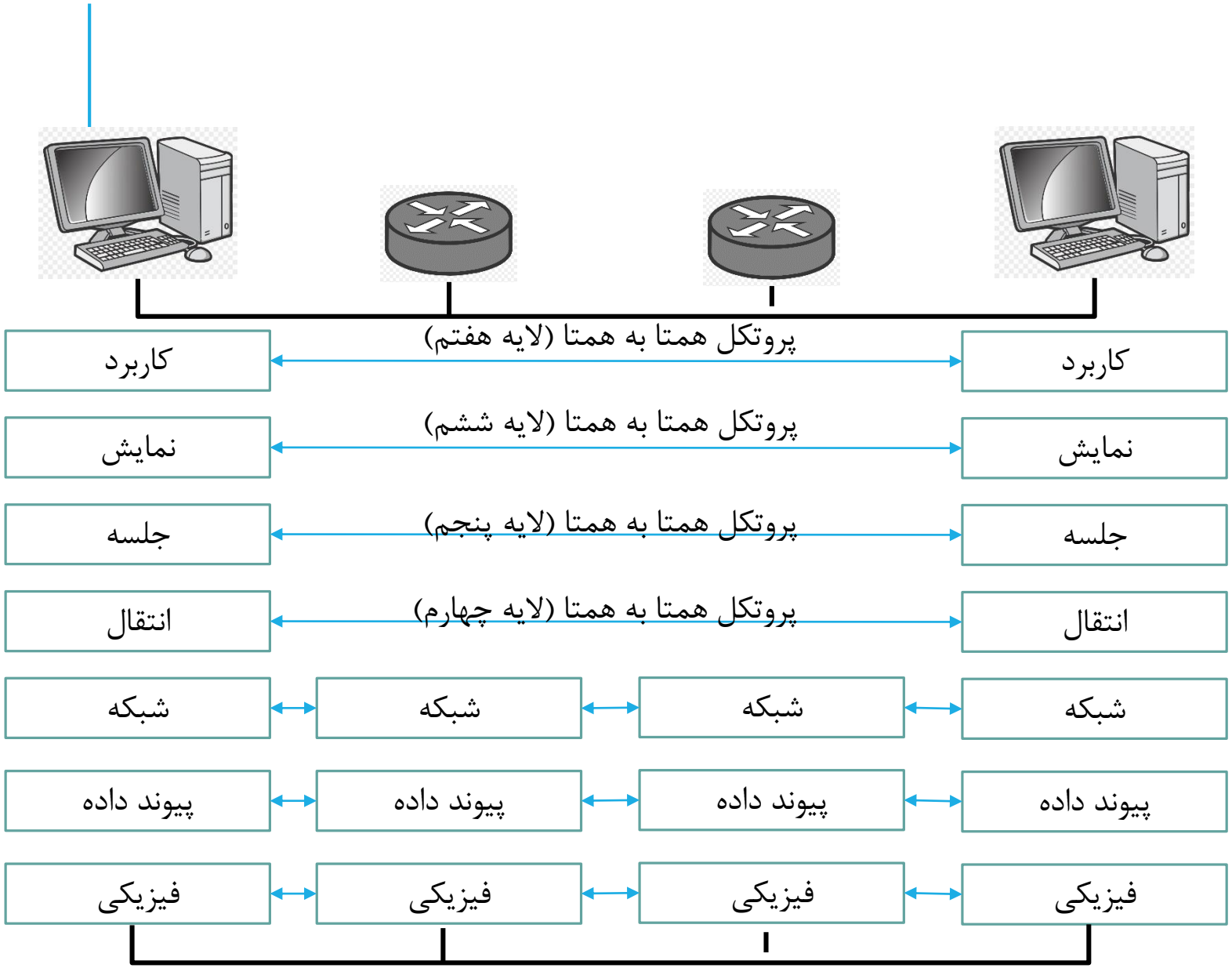
پیوند داده

فیزیکی

فرایندهای همتا-به-همتا

فرایندهایی که هر ماشین که در هر لایه با لایه متناظر ارتباط دارد.

استفاده از پروتکل‌های متناسب هر لایه


پروتکل همتا به همتا (لایه هفتم)
پروتکل همتا به همتا (لایه ششم)
پروتکل همتا به همتا (لایه پنجم)
پروتکل همتا به همتا (لایه چهارم)
کاربرد
نمایش
جلسه
انتقال
شبکه
پیوند داده
فیزیکی

پیاده‌سازی لایه‌ها

فیزیکی، پیونده و شبکه

- پشتیبانی شبکه
- نشانی فیزیکی حرکت داده از ابزاری به ابزار دیگر
- مشخصات الکتریکی، اتصالات فیزیکی
- نشانی‌دهی فیزیکی، زمان‌بندی انتقال، اطمینان

جلسه، نمایش، کاربرد

- پشتیبانی کاربر،
- اجراپذیری بین سیستم‌های نرم‌افزاری جدا از یکدیگر و بدون ارتباط

لایه انتقال

- پیوندها بین دو زیرمجموعه بالا

پیاده‌سازی لایه‌ها

رابط‌های خوش‌تعریف و کارکردهای لایه

- فراهم‌ساز ماژول‌بندی شبکه (انکپسولیشن)

لایه‌های پایین‌تر

- پیاده‌سازی از طریق سخت‌افزار و نرم‌افزار

لایه‌های بالاتر

- استفاده از نرم‌افزار

تبادل

کاربرد	داده ل۷
نمایش	اف۶ | داده ل۷
جلسه	اف۵ | داده ل۶
انتقال	اف۴ | داده ل۵
شبکه	اف۳ | داده ل۴
پیوند داده	اف۲ | داده ل۳ | اف۲
فیزیکی	00001000111010101000010000000

رسانه انتقال

لایه فیزیکی

توابع لازم جهت انتقال رشته بیت‌ها روی رسانه فیزیکی

نشانی‌دهی مشخصات مکانیکی و الکتریکی رابط و رسانه انتقال

تعریف کنندهٔ رویه‌ها و توابعی که جهت انجام انتقال

تعریف ویژگی‌های رابط بین ابزارها و رسانه انتقال

- نوع رسانه

نمایش بیتی

- کدکردن چگونگی تغییر صفرها و یک‌ها به سیگنال‌های یا الکترومغناطیسی یا نوری

تعریف آهنگ ارسال داده

- طول بیت

همگامی انتقال

لایه فیزیکی

پیکربندی خط

- نقطه به نقطه: پیوند اختصاصی
- چندنقطه‌ای: شراکت چند ابزار روی پیوند

توپولوژی فیزیکی

- چگونگی صورت اتصال ابزارها و تشکیل شبکه
  - ستاره‌ای، حلقوی، باس
- نوع انتقال
  - یک‌طرفه
  - نیمه دوطرفه
  - دوطرفه کامل

لایه پیوند داده

لایه فیزیکی

- ابزار انتقال ساده و ابتدایی

تبدیل لایه فیزیکی به پیوندی مطمئن

بی‌خطا نشان دادن لایه فیزیکی به لایه‌های بالاتر

لایه پیوند داده- کارها

قاب‌بندی
- تبدیل رشته بیت‌ها به واحدهای داده مدیریت‌پذیر

نشانی‌دهی فیزیکی
- افزودن سر جهت مشخص کردن فرستنده و گیرنده

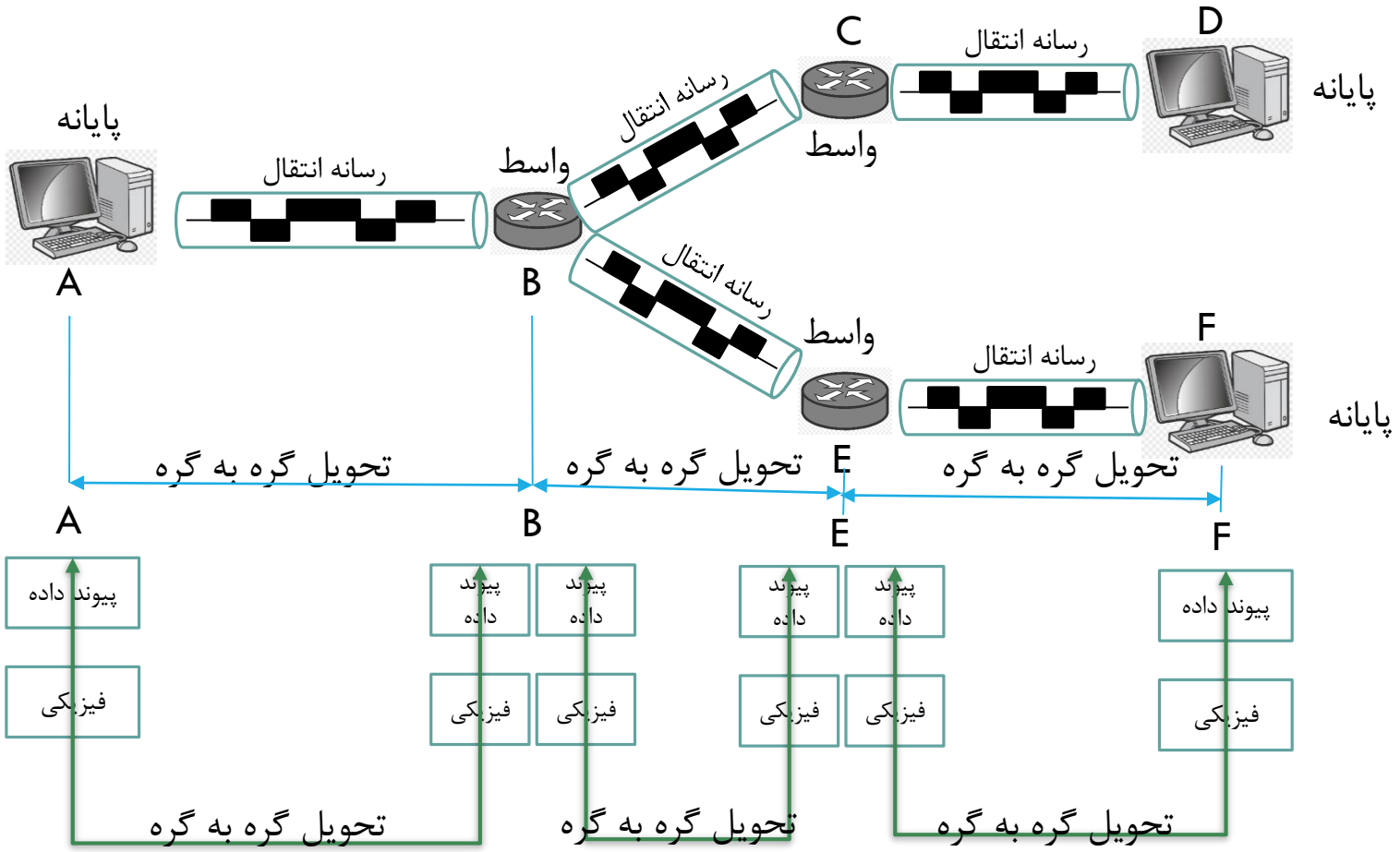
کنترل جریان
- اعمال مکانیسم کنترل هنگام کندتر بودن گیرنده از فرستنده

کنترل خطا
- صاحب سازوکارهایی جهت تخشخیص و بازانتقال قب‌های آسیب‌دیده یا گم شده
- چلوگیری از تکرار قاب‌ها

کنترل دسترسی
- در پیکربندی چندنقطه‌ای
- نیاز به سازوکاری جهت مشخص کردن تخت اختیار داشتن پیوند در هر زمان

تحویل گره به گره

لایه پیوند داده- کارها



لایه شبکه

مسئول تحویل دادهٔ (بسته) مبدا به مقصد در طول چند پیوند شبکه‌ای

اطمینان از دریافت بسته‌ها در مقصد از مبدا

عدم نیاز به لایه شبکه در صورتی که دو سیستم با یک پیوند متصل باشند

نیاز به لایه شبکه در صورتی که دو سیستم متصل به پیوندهای متفاوت (شبکه‌ها) باشند

- جهت انجام تحویل مبدا به مقصد

لایه شبکه- کارها

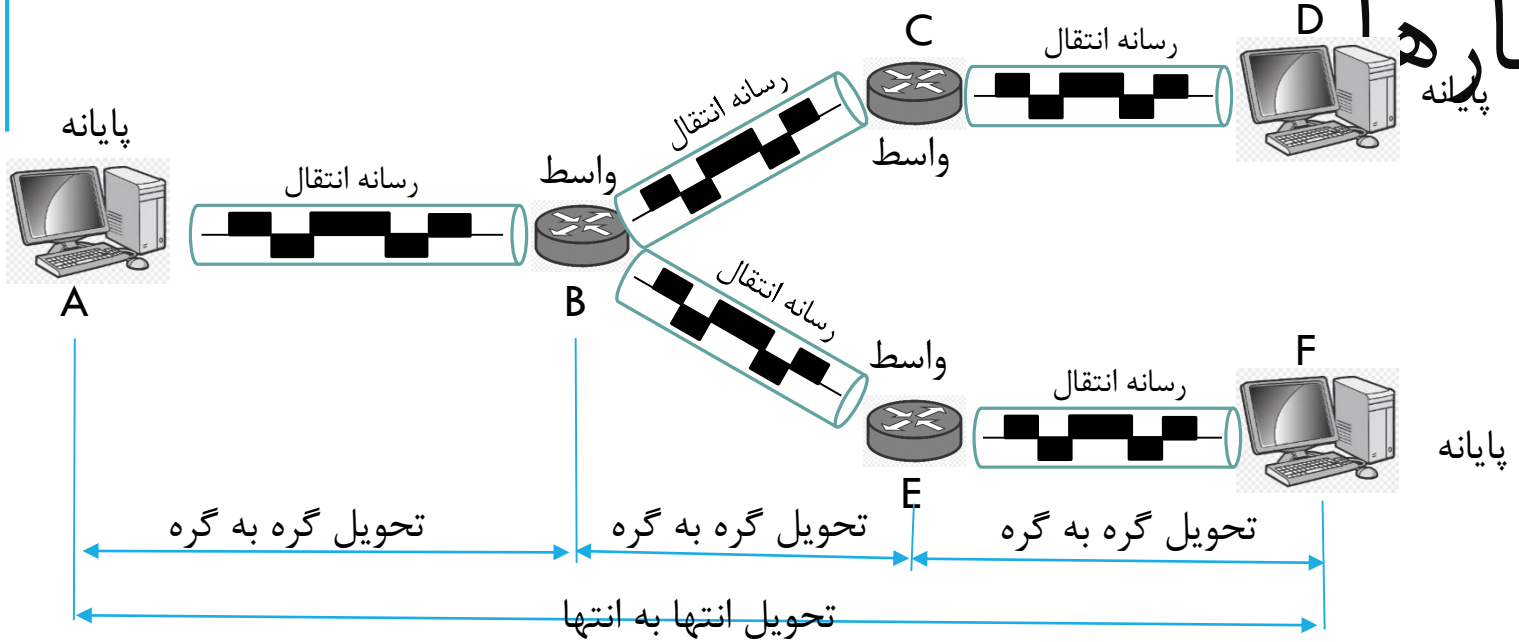
نشانی‌دهی منطقی

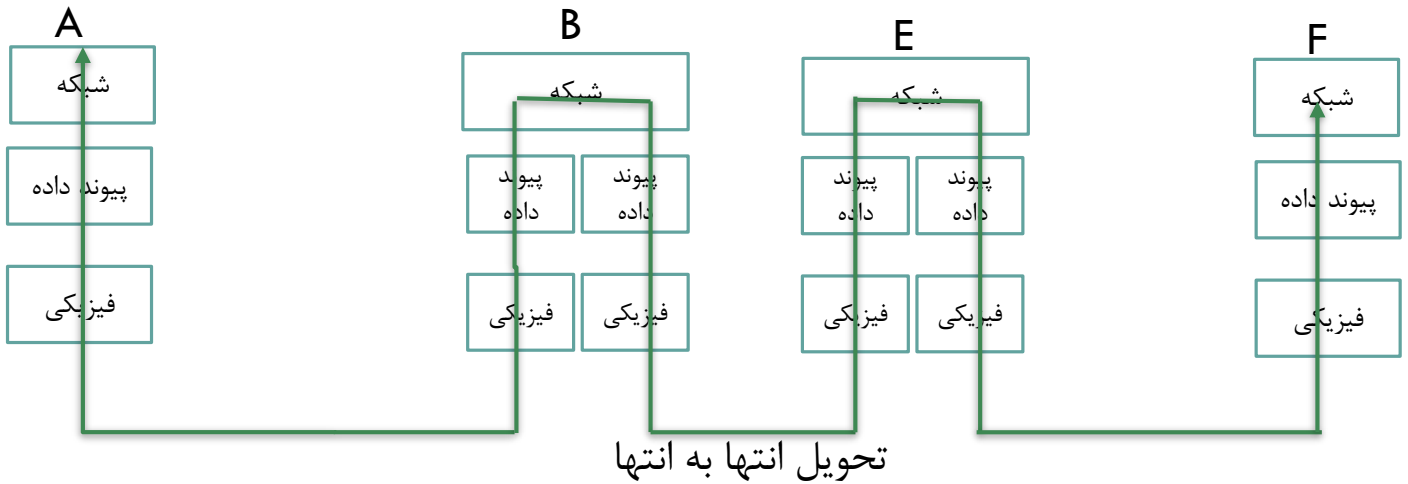
- نشانی‌دهی فیزیکی ل‌پ‌د صرفا نشانی‌دهی محلی
- نیاز به نظام نشانی‌دهی دیگر در قرارگیری مقصد در شبکه‌ای متمایز (گذر از مرزهای شبکه)
- افزودن نشانی منطقی سربند فرستنده و گیرنده

مسیریابی

- ترکیب شبکه‌ها و پیوندها و تشکیل شبکه‌هایی از شبکه‌ها (بین‌شبکه‌ها)
- ابزارهای متصل منجر به ارسال بسته‌ها به مقصد نهائی
- تابع لایه شبکه جهت ممکن‌سازی چنین سازوکاری

لایه شبکه- کارها ۱





لایه انتقال

مسئول تحویل مبدا به مقصد (انتها به انتهای) کل پیام

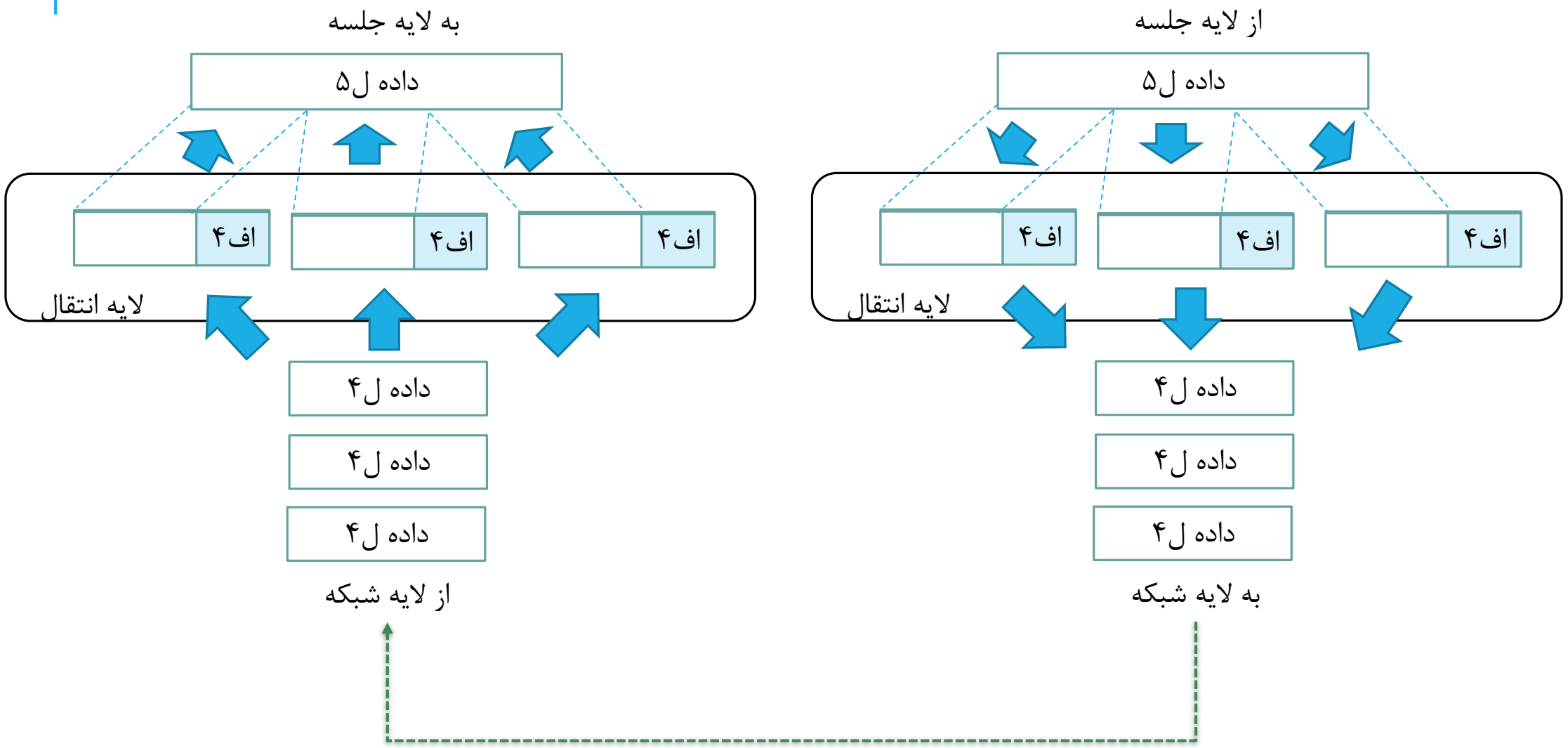
تفاوت با لایه شبکه

- مسئول تحویل انتها به انتهای هر بستهٔ منفرد
- عدم شناسایی رابطه بین بسته‌ها
- شناخت هر بسته به عنوان پیامی مجزا فارغ از درستی چنین نگاهی

اطمینان از تحویل کامل و مرتب تمامی پیام (مجموعه بسته‌ها)

نظارت بر کنترل خط و کنترل جریان در سطح مبدا به مقصد

لایه انتقال


از لایه جلسه
داده ل۵
اف۴
اف۴
اف۴
لایه انتقال
داده ل۴
داده ل۴
داده ل۴
به لایه شبکه
به لایه جلسه
داده ل۵
اف۴
اف۴
اف۴
لایه انتقال
داده ل۴
داده ل۴
داده ل۴
از لایه شبکه

لایه انتقال- وظایف

نشانی‌دهی درگاه پورت خدمت

- محدویت ابزار به ابزار به جهت اینکه ابزارها چند فرایند را که امکان ارتباط به فرایندهای ابزارهای دیگر دارند پشتیبانی می‌کنند.
- لایه انتقال نشانی‌دهی خدمت خدمت
- لایه شبکه اطمینان از دریافت بسته در مقصد
- لایه انتقال گرفتن کل پیام به فرایند متناظر در رایانه

قطعه‌بندی و سرهم‌بندی

- تقسیم پیام به قطعات انتقال‌پذیر
- هر یک با شماره ترتیب
- سرهم‌بندی پیام‌ها و مشخص کردن بسته‌های گم‌شده در انتقال و تعویض آنها

کنترل اتصال

- اتصال‌محور یا بی‌اتصال
- اتصال‌محور اندرکنش بیشتر مبدا و مقصد
- درخواست اتصال فرستنده قبل ارسال بسته
- بستن اتصال پس از ارسال همه بسته‌ها

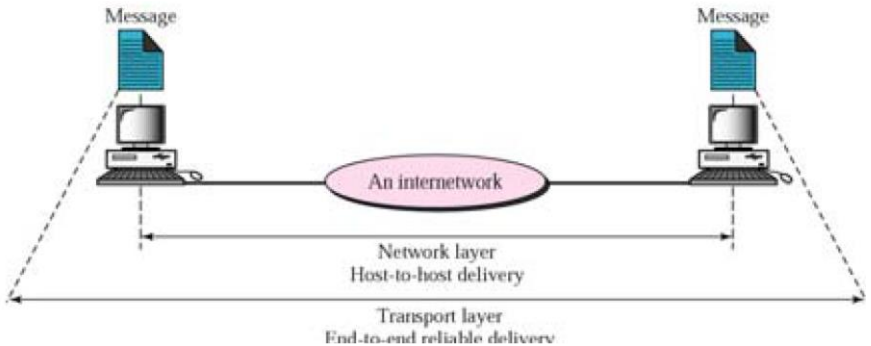
لایه انتقال- وظایف

کنترل جریان

- همانند لایه پیوند داده
- اعمال کنترل جریان در سطح انتها به انتها به جای سطح تک پیوند

کنترل خطا

- همانند لایه پیوند داده مسئول کنترل خطا
- انتها به انتها
- اطمینان از دریافت کل پیام بدون آسیب یا گم‌شدگی یا افزونگی و تکرار
- انجام تصحیح معمولا با ارسال دوباره



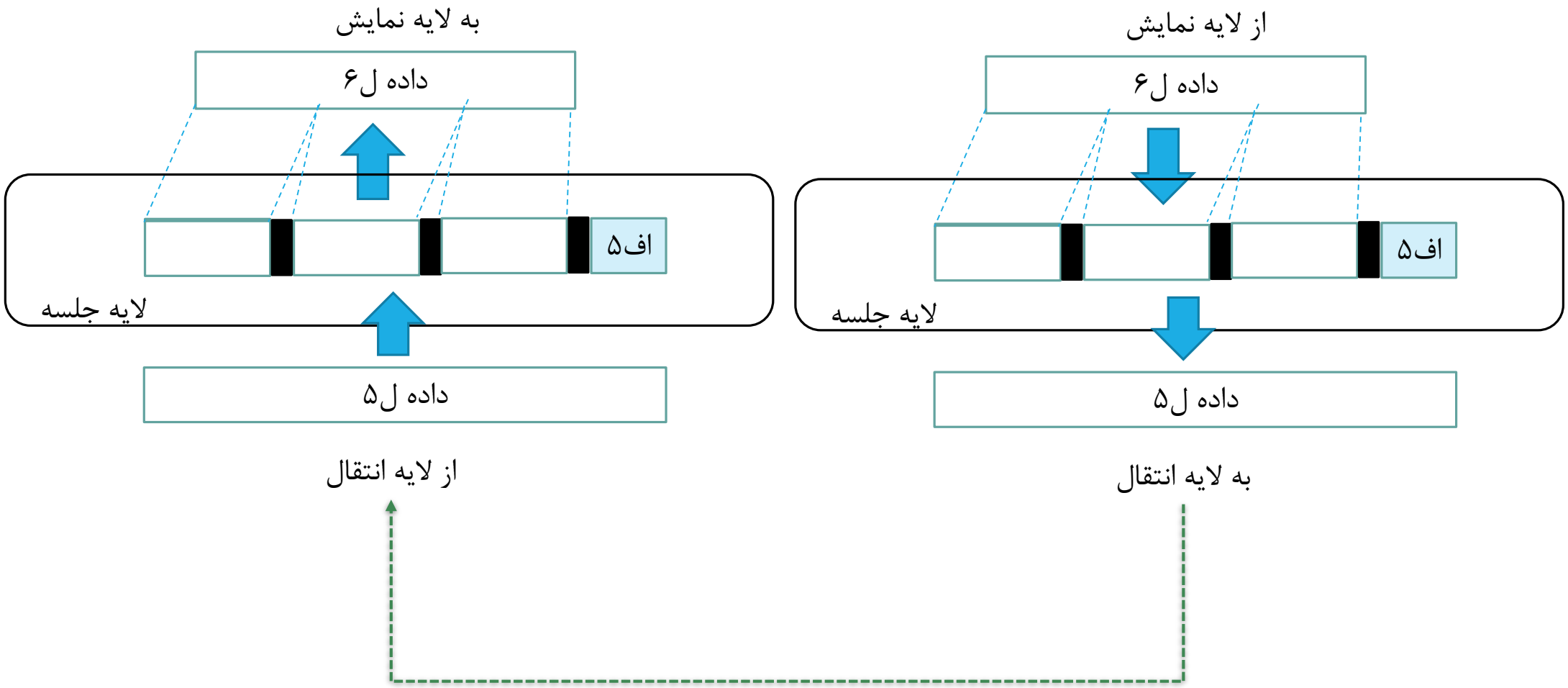
لایه جلسه

کنترل‌گر مفاوضه و دیالوگ در شبکه

اجازه ایجاد ارتباط بین دو سیستم

- مدهای کنترل دوطرفه، نیمه دوطرفه
- اجازه به فرایندها برای افزودن نقاط وارسی به جریان داده
  - نقاط همگامی
- امکان بازیابی شکستی در انتقال پیام بدون نیاز به ارسال دوبارهٔ کل پیام

لایه جلسه


از لایه نمایش
داده ل۶
اف۵
لایه جلسه
داده ل۵
به لایه انتقال
به لایه نمایش
داده ل۶
اف۵
لایه جلسه
داده ل۵
از لایه انتقال

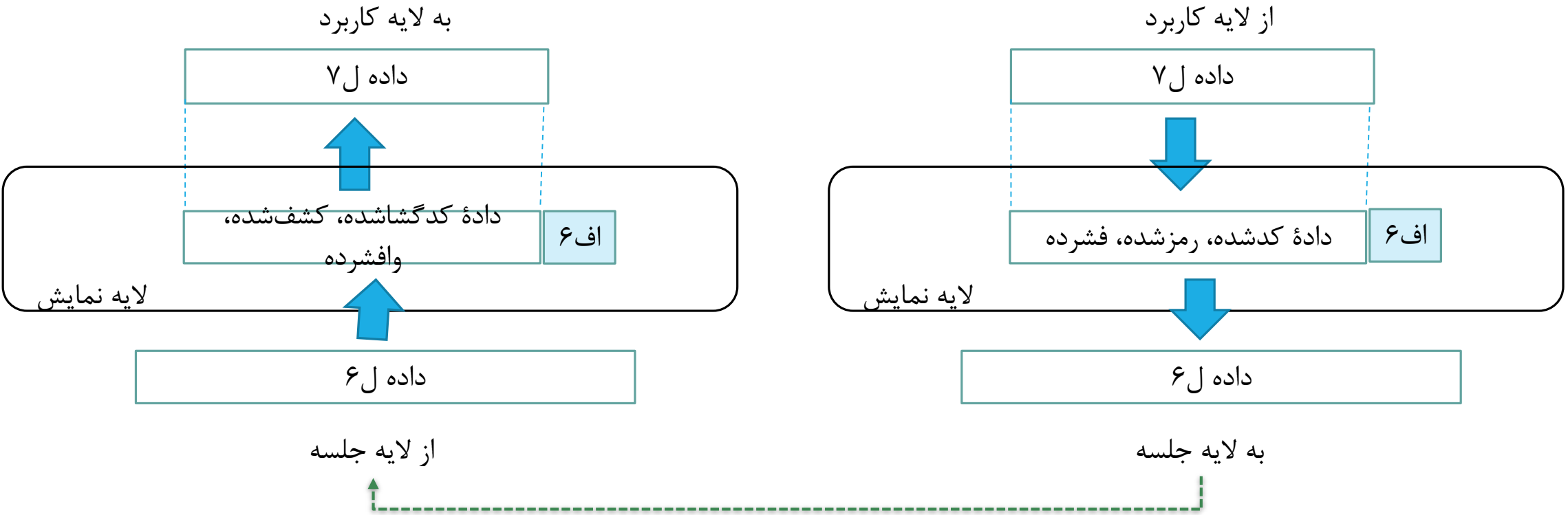
لایه نمایش

درگیر نحو و معنای اطلاع تبادلی بین دو سیستم

وظایف

- ترجمه
  - حل کردن نمایش‌های عددی و نویسه‌های متفاوت
- کدگذاری
- فشرده‌سازی
  - مهم برای داده‌های چندرسانه‌ای

لایه نمایش


از لایه کاربرد
داده ل۷
داده کدشده، رمزشده، فشرده
اف۶
لایه نمایش
داده ل۶
به لایه جلسه
به لایه کاربرد
داده ل۷
داده کدگشاشده، کشف‌شده، وافشرده
اف۶
لایه نمایش
داده ل۶
از لایه جلسه

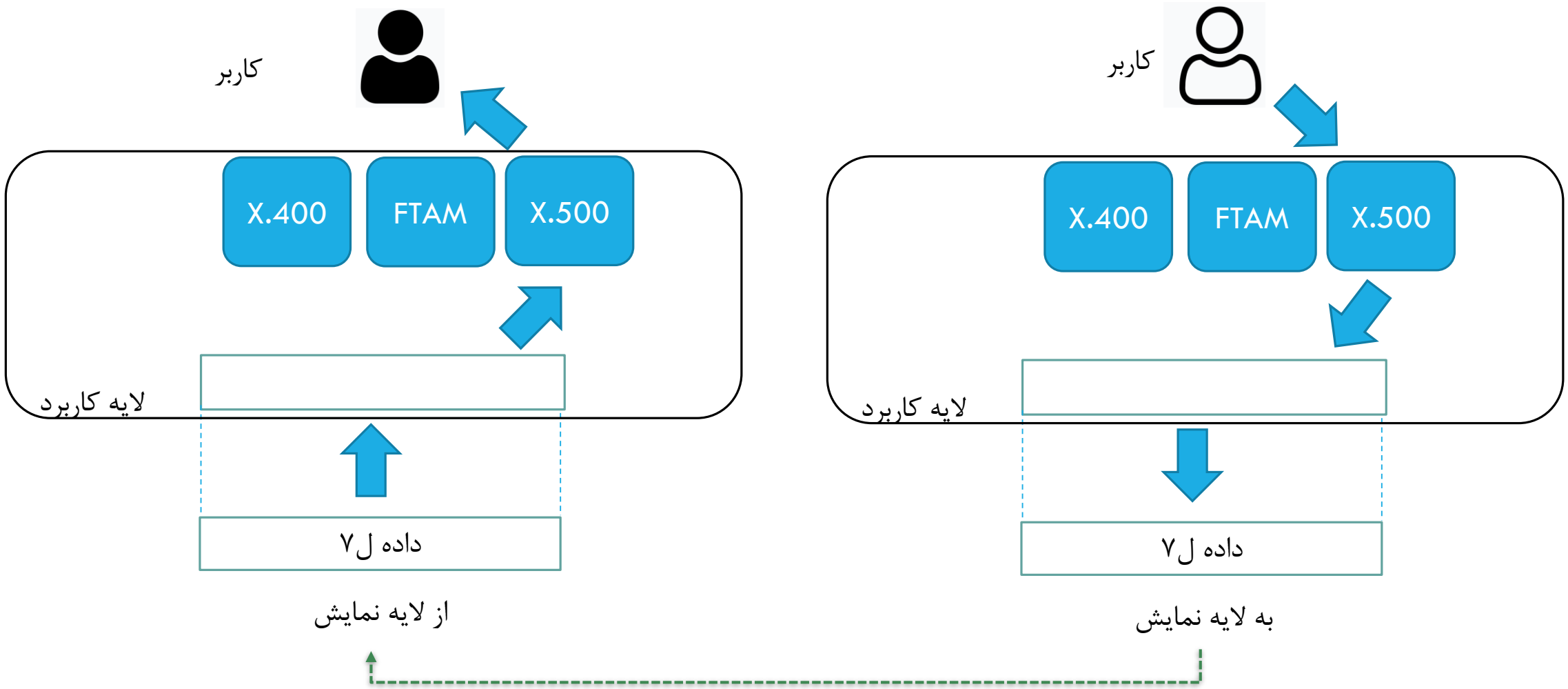
لایه کاربرد

امکان‌دهی به کاربر جهت کار مستقیم با نرم‌افزار کاربردی جهت دسترسی به شبکه

فراهم کردن واسطهای کاربری و پشتیبانی از خدماتی چون

- خدمات ای-نامه
- دسترسی به فایل دور و انتقال FTP و HTTP
- خدمات دایرکتوری DNS پایگاه داده‌های توزیعی
- ترمینل مجازی شبکه Telnet
- ابزارهای مخرب

لایه کاربرد


کاربر
X.400
FTAM
X.500
لایه کاربرد
داده ل۷
به لایه نمایش
کاربر
X.400
FTAM
X.500
لایه کاربرد
داده ل۷
از لایه نمایش

خلاصه لایه‌ها

کاربرد
- اجازهٔ دسترسی به منابع شبکه

نمایش
- ترجمه،کد کردن، فشردن داده

جلسه
- برقراری، مدیریت، و اتمام جلسات

انتقال
- ممکن‌سازی تحویل پیام فرایند به فرایند مطمئن و بازیابی خطا

شبکه
- ارسال بسته‌ها از مبدا به مقصد
- امکان بین‌شبکه‌کاری

پیوند داده
- سازماندهی بیت‌ها در قالب قاب‌ها
- تحویل گام به گام

فیزیکی
- ارسال بیت روی رسانه
- مشخص کردن مشخصات مکانی و الکتریکی

پروتکل TCP/IP

ایجاد پیش از مدل OSI

پنج لایه به جای هفت لایه

- تعریف پروتکل‌ها برای سه لایه

لایه کاربرد TCP شامل لایه‌های نمایش و جلسه مدل OSI

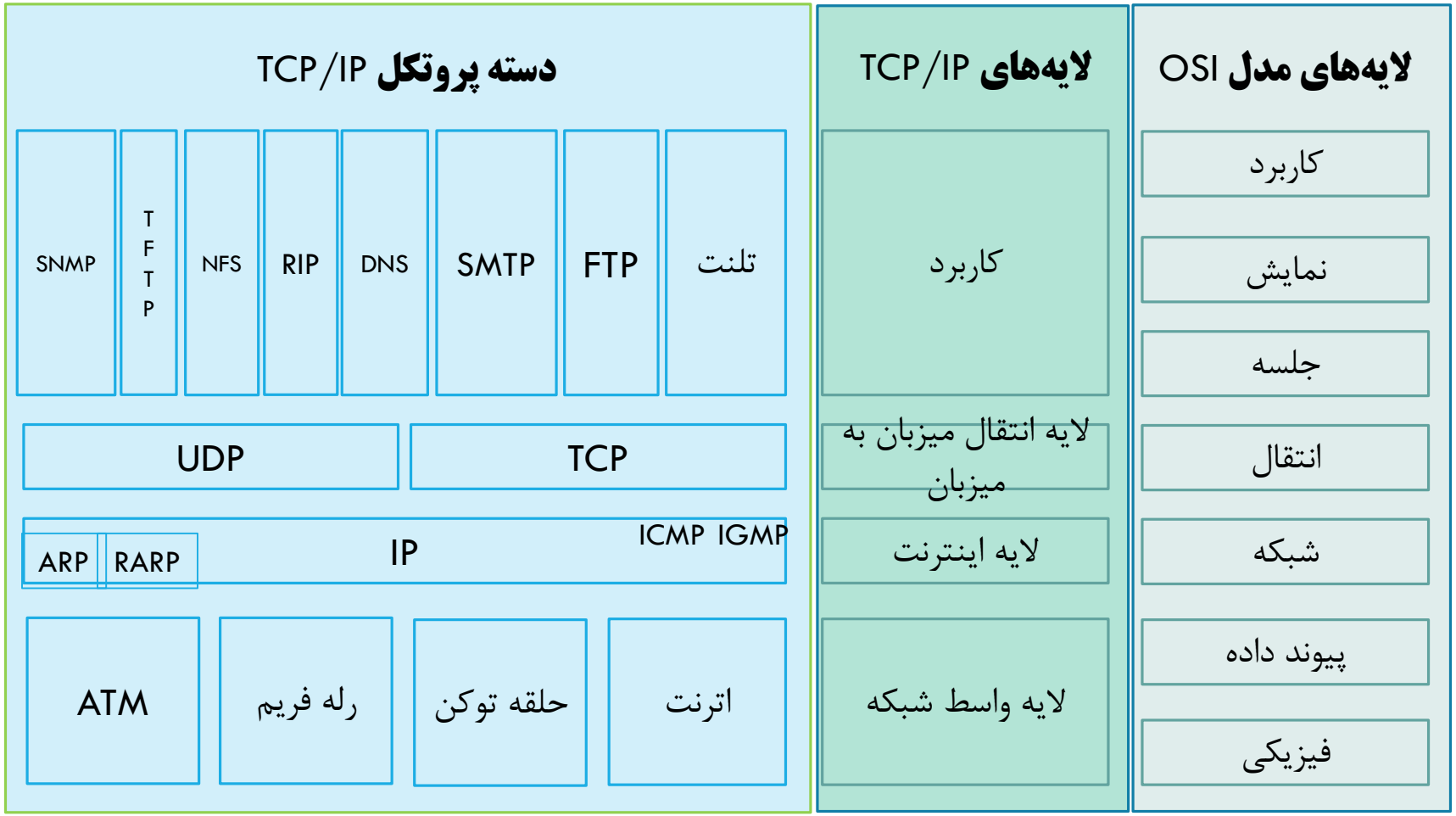
لایه انتقال شامل دو پروتکل

- TCP
- UDP

لایه شبکه: پروتکل بین‌شبکه‌کاری Internetworking Protocol IP

- Internet Control/Group Message Protocol
- (Reverse) Address Resolution Protocol

مدل OSI و TCP/IP



لایه (بین)شبکه

پروتکل اینترنت

- IP
- بدون اطمینان و بی‌اتصال
- بدون وارسی خط و رهگیری
- بسته‌های آی‌پی: دیتاگرم
- ارسال جداگانه و امکان سفر از مسیرهای متفاوت
- امکان دریافت خارج از ترتیب و دریافت چندباره
- عدم رهگیری مسیرها و عدم امکان بازترتیب بسته‌ها
- اجازه افزودن توابع و کارکردهای جدید در صورت لزوم

لایه (بین)شبکه

Address Resolution Protocol (ARP)

- ARP(IP_Address) → Physical_Address
- RARP(Physical_Address) → IP_Address

Internet Control Message Protocol (ICMP)

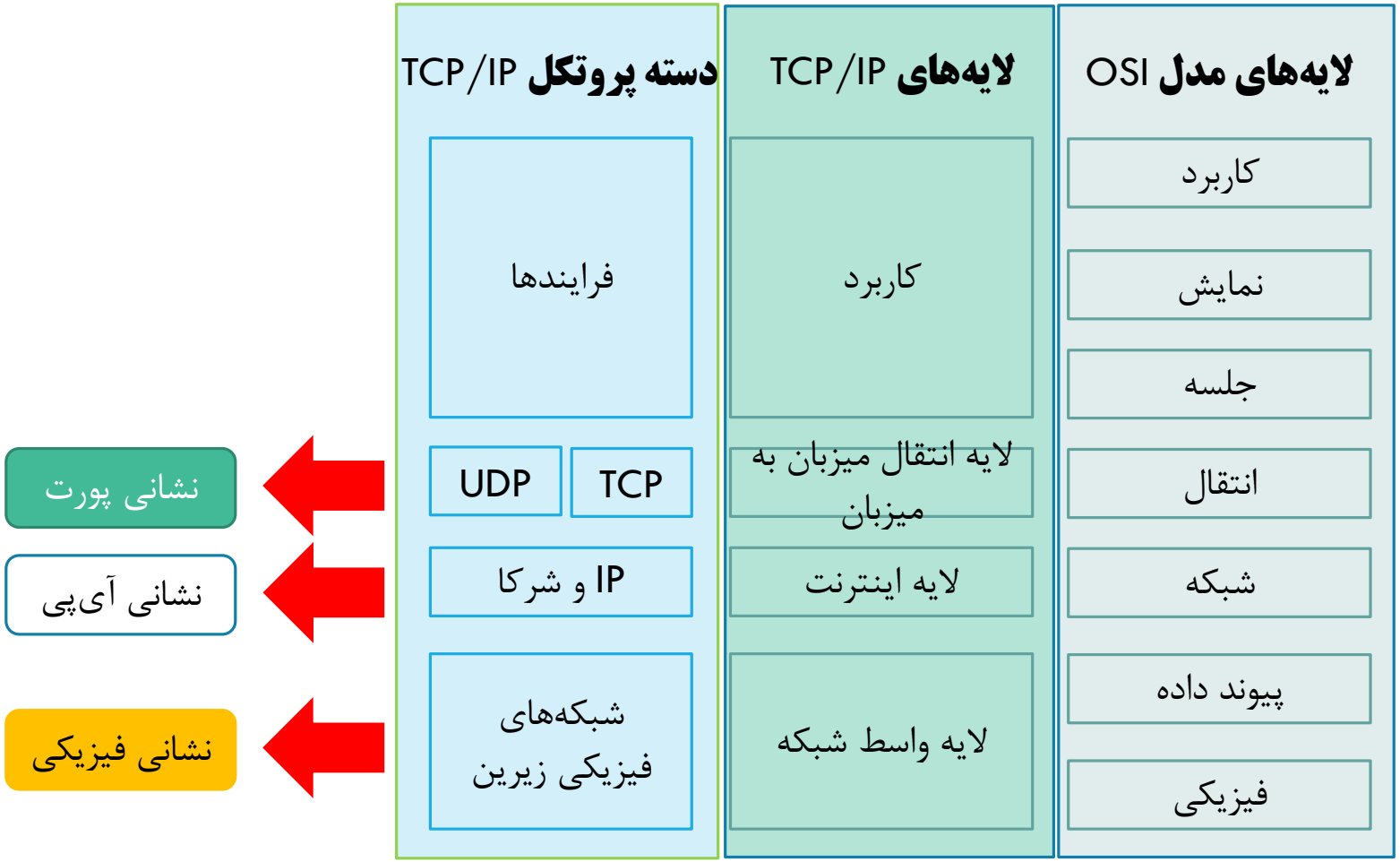
- گزارش خطا

Internet Group Message Protocol (IGMP)

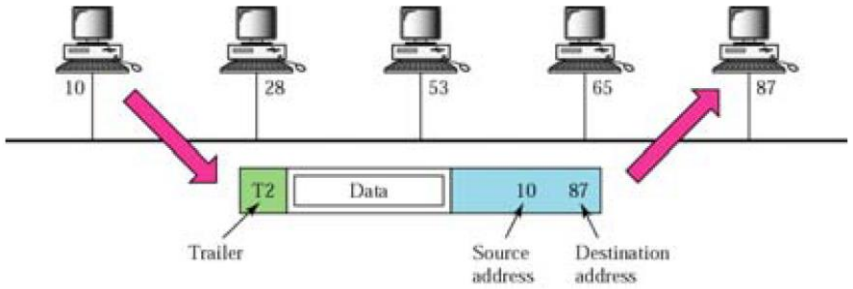
- مدیریت چندارسالی

نشانی‌دهی در TCP/IP

نشانی‌ها
- نشانی فیزیکی
- نشانی IP
- نشانی درگاه یا پورت



مفهوم نشانی فیزیکی

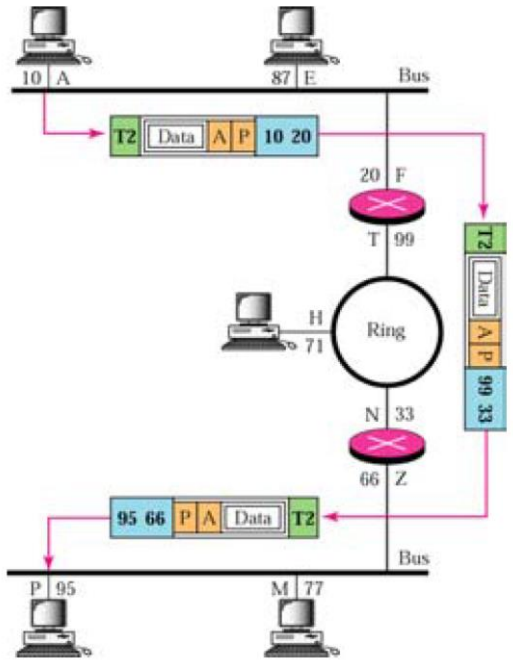


نشانی‌دهی فیزیکی

بیشتر شبکه‌های محلی

- نشانی ۴۸ بیتی یا شش بایتی
- نمایش با ۱۲ رقم شانزدگانی
- هر دو بایت جداشده با خط
- 07-01-02-01-2C-4B

نشانی‌دهی IP

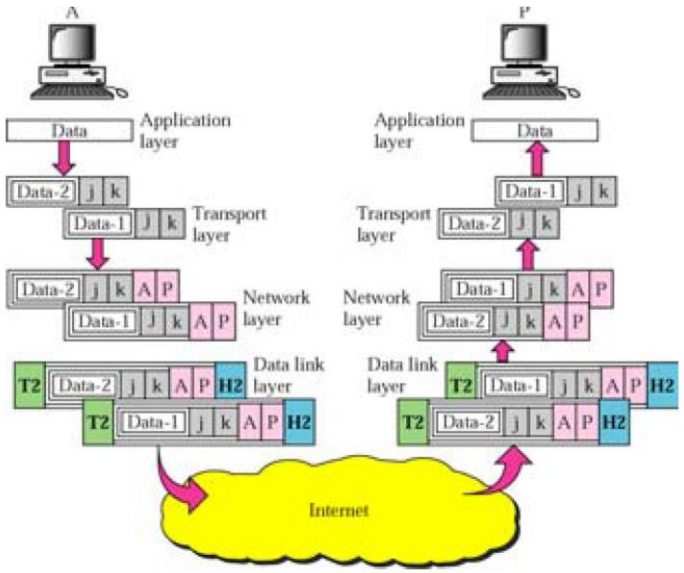

10 A
87 E
Bus
T2 Data A P 10 20
20 F
T 99
H
71
Ring
N 33
66 Z
95 66 P A Data T2
Bus
P 95
M 77
T2
Data
A
P
99 33

نشانی‌دهی IP

نشانی اینترنت

- IPv4
- ۳۲ بیت در طول
- نمایش معمول با چهار عدد دهگانی
- هر یک نمایش یک بایت و جداسازی با نقطه
- 168.172.75.9

نشانی‌دهی پورت



نُسَخ TCP/IP

نسخهٔ ۴-

نسخهٔ ۵- با IPv6 جانشین شد

نسخهٔ ۶

- به کارگیری در امریکا
- بکارگیری در بسیاری کشورها

منابع

Forouzan, “TCP/IP Protocol Suite” (2nd Edition)