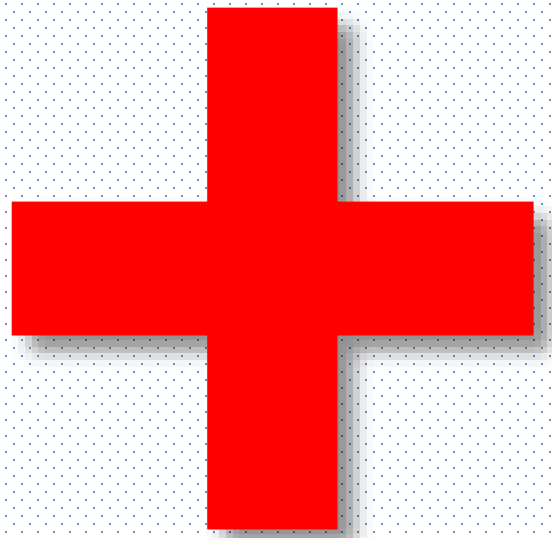
NETWORK



آشنایی با:

- شبکه و اجزای آن
- توپولوژی و انواع آن
- انواع کابل شبکه
- ابزار شبکه
- تجهیزات شبکه
- مقیاس شبکه
- مدل مرجع OSI و هفت لایه آن
- پروتکل
- IP Address
- دستورات شبکه در CMD
- امنیت شبکه
- شبکه وایرلس

شبکه (Network):

سیستمی از اشیاء یا اشخاص متصل به یکدیگر برای عمل انتقال

شبکه های کامپیوتری

شبکه های حمل و نقل

شبکه های اجتماعی

اجزای سخت افزاری شبکه های کامپیوتری:

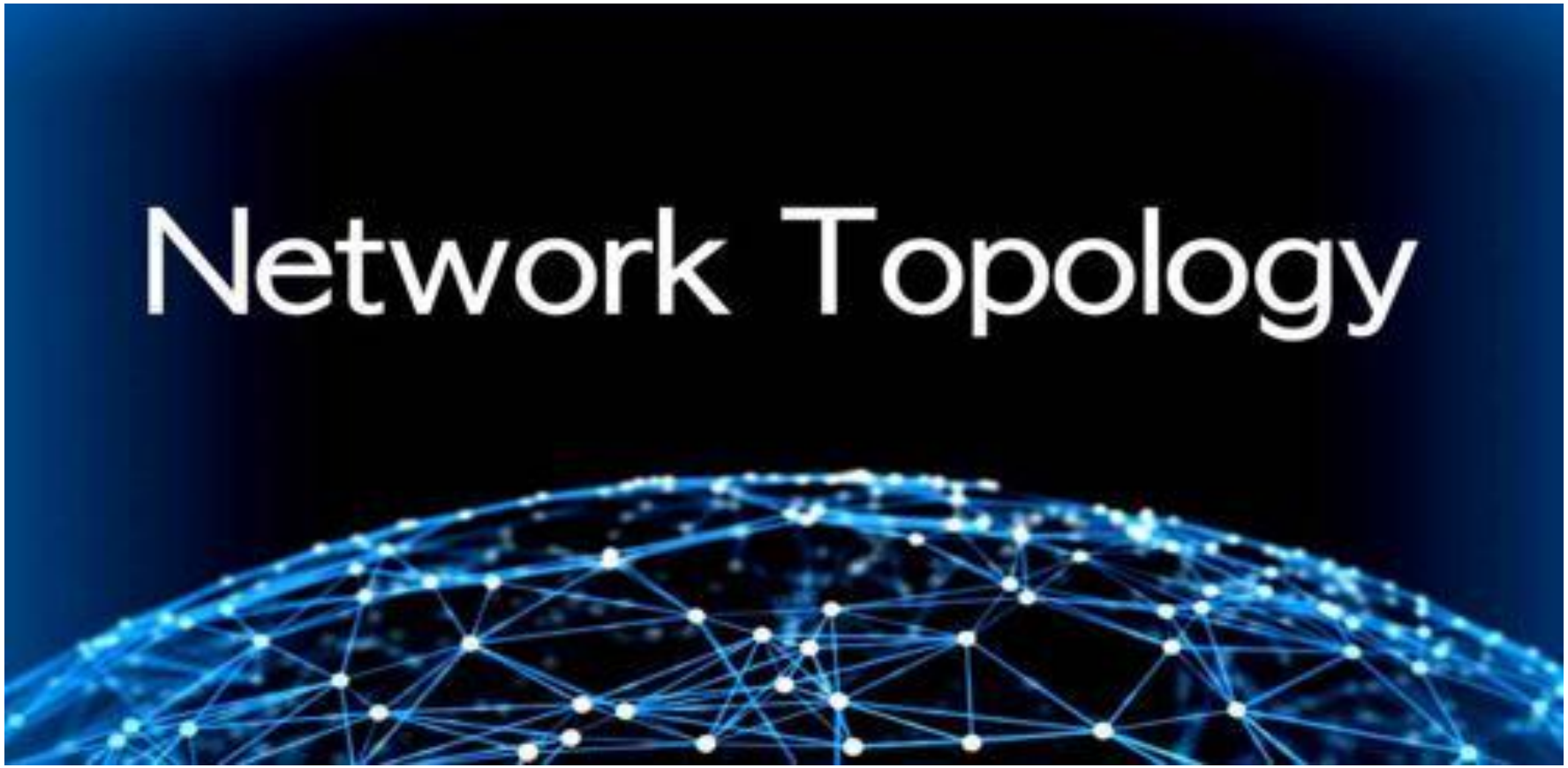
1- میزبان (Host) ← Node

2- واسط میانی (Interface)

3- رسانه انتقال (Link) ← جهت ارتباط Node ها

توپولوژی (Topology) چیست؟

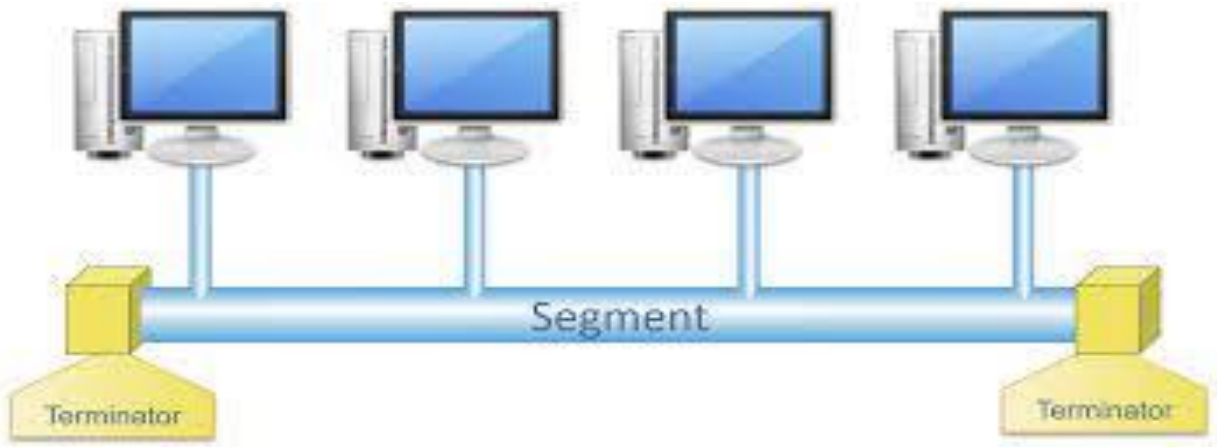
چگونگی اتصال واقعی Node ها به یکدیگر توسط رسانه انتقال



انواع توپولوژی ها:

❖ BUS

✓ اتصال تمامی کامپیوترها به یک کانال مشترک



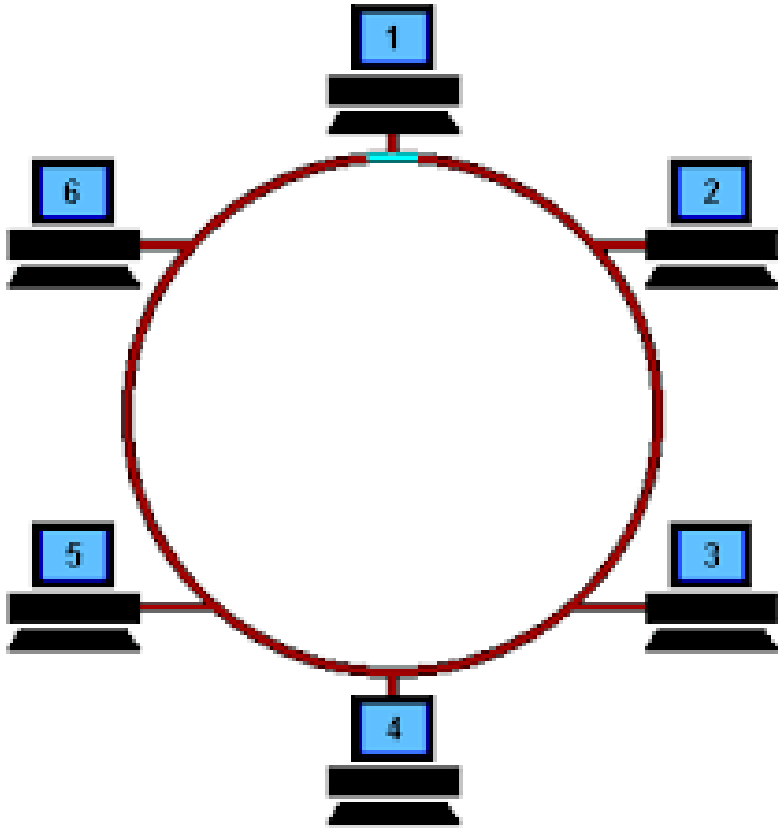
مزایا و معایب:

- راه اندازی ساده و هزینه ارزان آن
- قطع شدن شبکه در صورت خرابی کانال
- محدود بودن تعداد کامپیوترها
- مشکل بودن خطایابی و رفع اشکال شبکه

انواع توپولوژی ها:

❖ RING

✓ اتصال تمامی کامپیوترها به صورت نقطه به نقطه از طریق یک حلقه

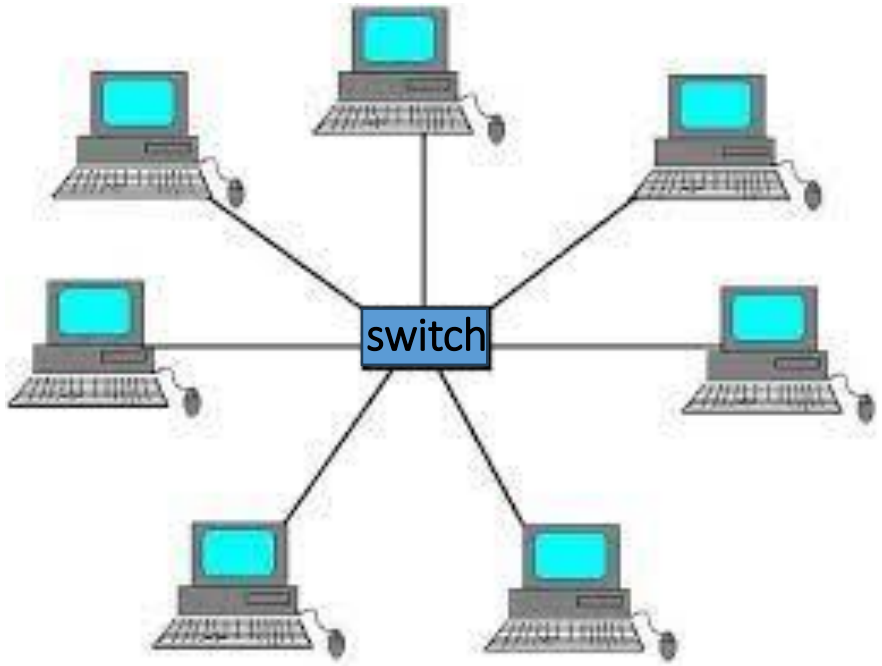


مزایا و معایب:

- عدم تضعیف سیگنال در انتقال
- جهت انتقال اطلاعات یک طرفه است

انواع توپولوژی ها: ❖ STAR

✓ اتصال تمامی کامپیوتر ها به یک ایستگاه مرکزی

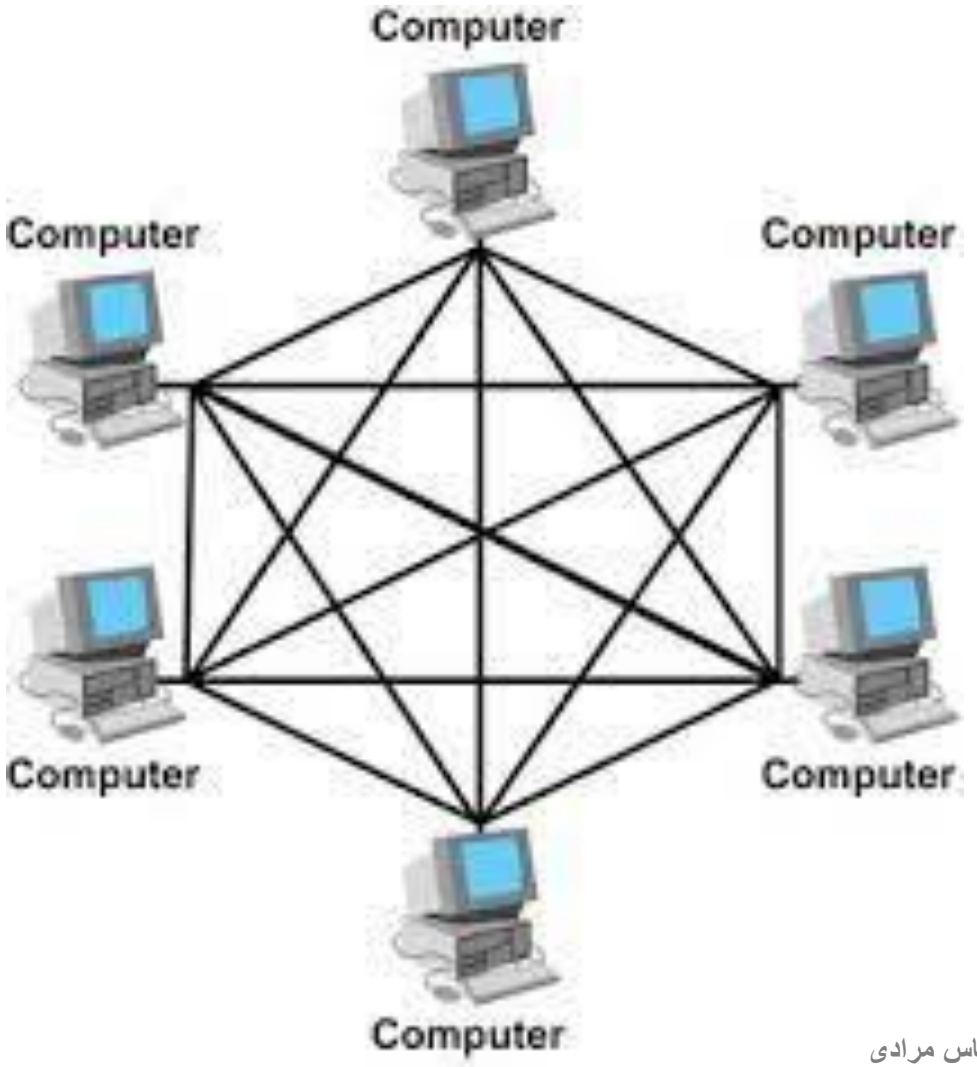


مزایا و معایب:

- با خرابی کانال، شبکه از کار نمی افتد
- قابلیت گسترش نسبتا آسان
- سرعت به نسبت بالا
- هزینه بالا، مقدار کابل زیادی استفاده می شود
- در صورت خرابی سویچ ،شبکه از کار می افتد

انواع توپولوژی ها:

❖ MESH

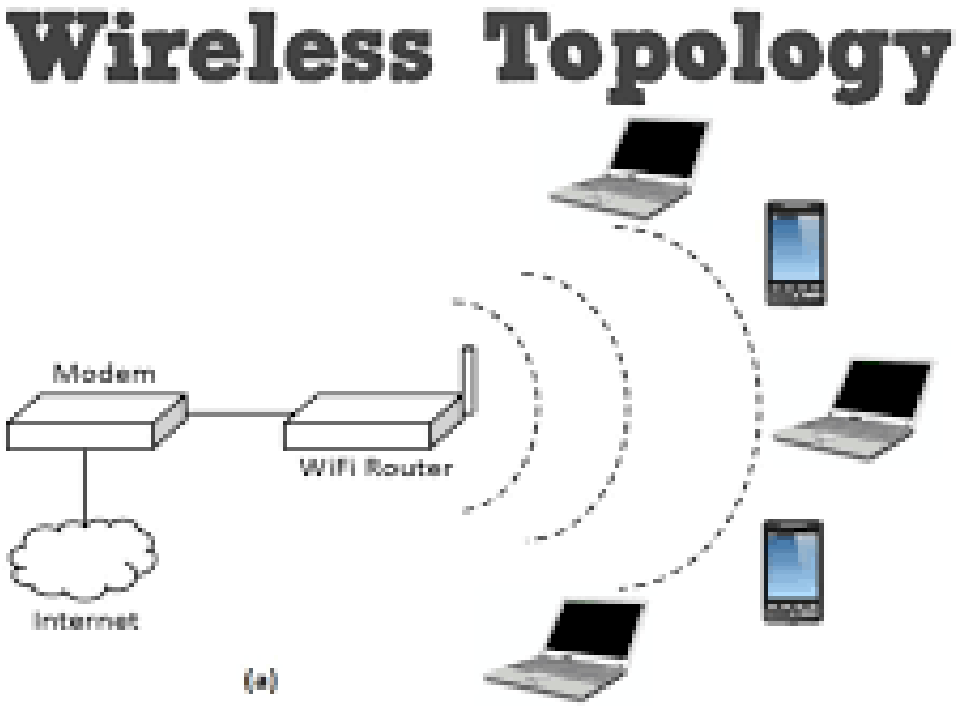


مزایا و معایب:

- سرعت انتقال داده بالا
- قابلیت اطمینان بالا
- عدم وجود مشکل ترافیک در شبکه
- هزینه بسیار بالا بدلیل تعداد کانال بسیار زیاد
- قابلیت گسترش شبکه مشکل است

انواع توپولوژی ها:

❖ Wireless



مزایا و معایب:

- هزینه پایین بدلیل عدم وجود کابل
- قابلیت گسترش شبکه آسان است
- قابلیت اطمینان پایین
- سرعت پایین

معیار مقاسیه توپولوژی ها:

- سرعت
- قابلیت اطمینان
- هزینه
- سهولت در قابلیت گسترش

توپولوژی رایج:

انواع کابل:

COAXIAL

- THIN ← 185 M
- THICK ← 500 M

DVR

BNC Connector

انواع کابل:

Single Mode ⟵ فاصله های طولانی تا چندین هزار متر

Multi Mode ⟵ فاصله های کوتاه 400-300 متر

FIBER OPTIC ❖

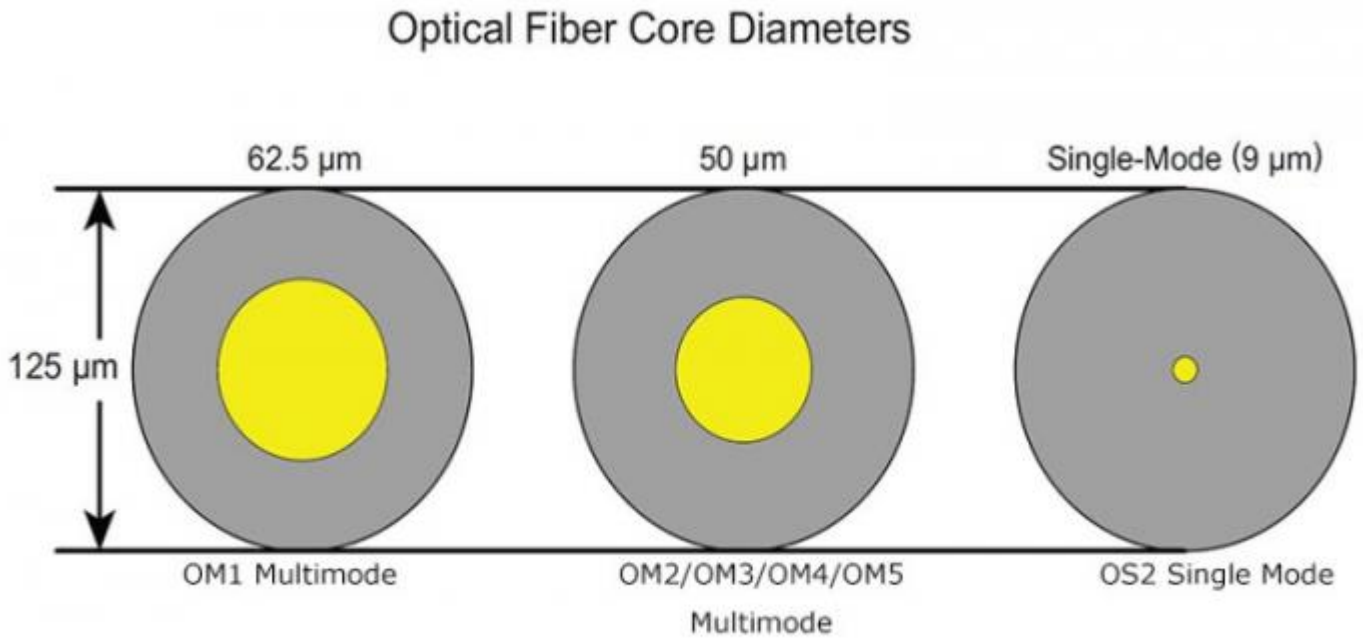


Figure 1: Optical Fiber Core Diameters

انواع کابل:

- پچ پنل:

❖ تجهیزات فیبر نوری:

- پیگتیل:

انواع کابل:

- آداپتور:

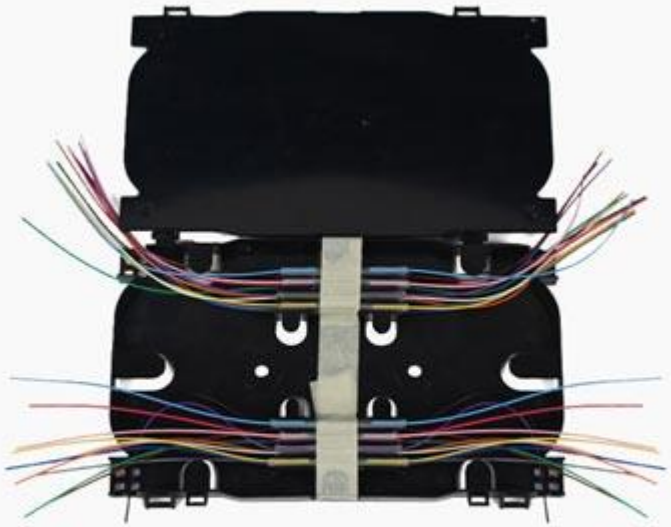
❖ تجهیزات فیبر نوری:

- پچ کورد:

انواع کابل:

- کیبل منیجمنت:

❖ تجهیزات فیبر نوری:



- کاست:

انواع کابل:

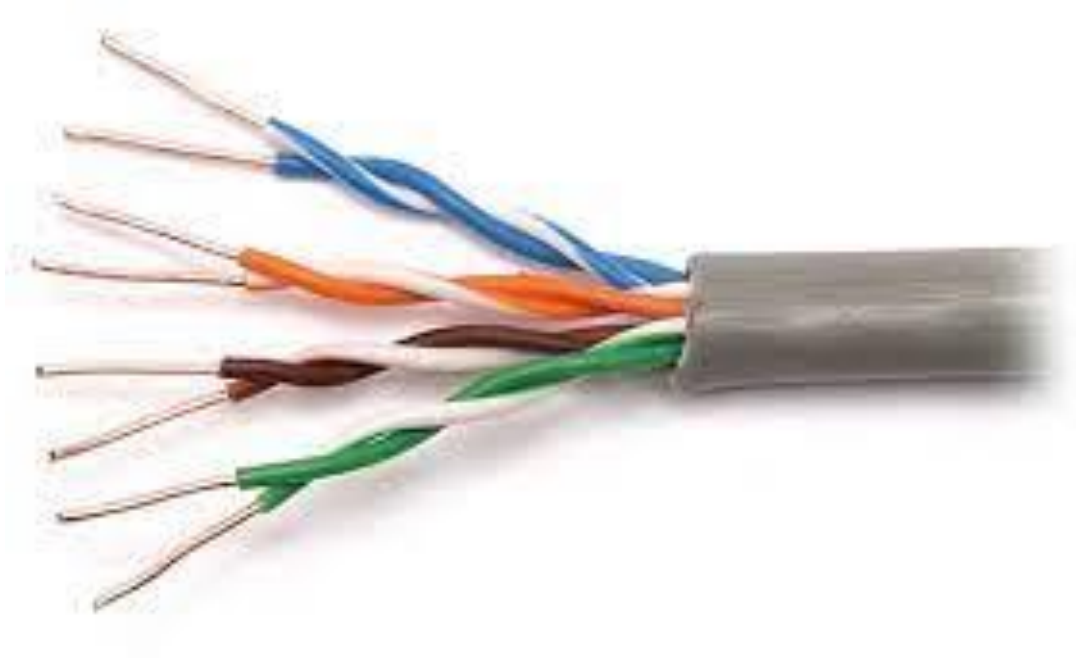
TWISTED PAIR

UTP ← بدون شیلد

STP ← شیلد دار

RJ45

Keystone

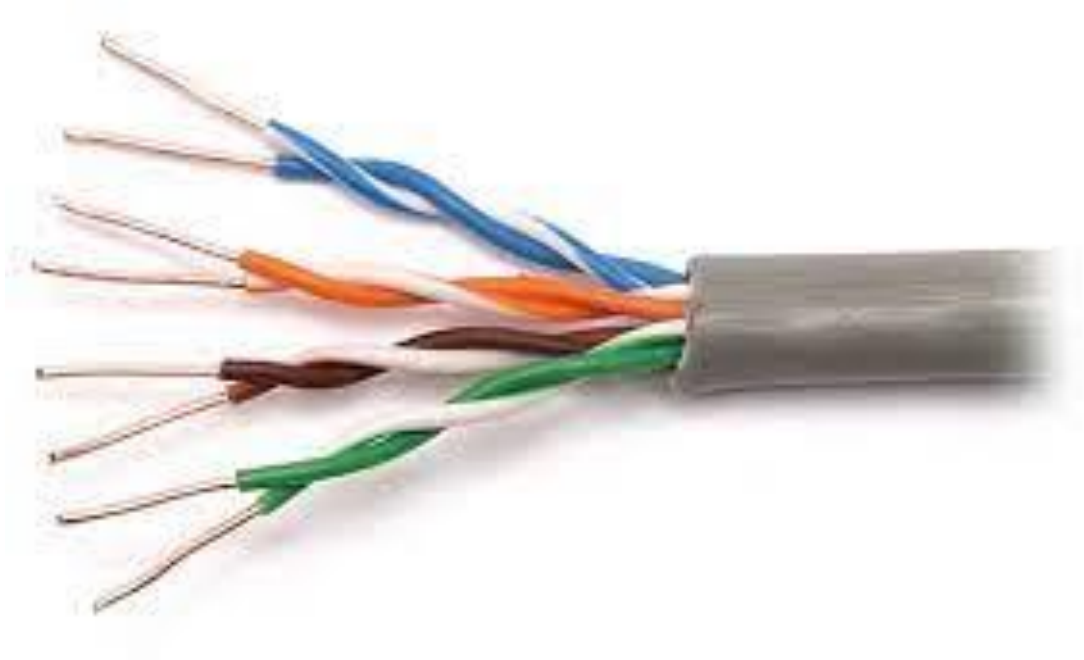


انواع کابل:

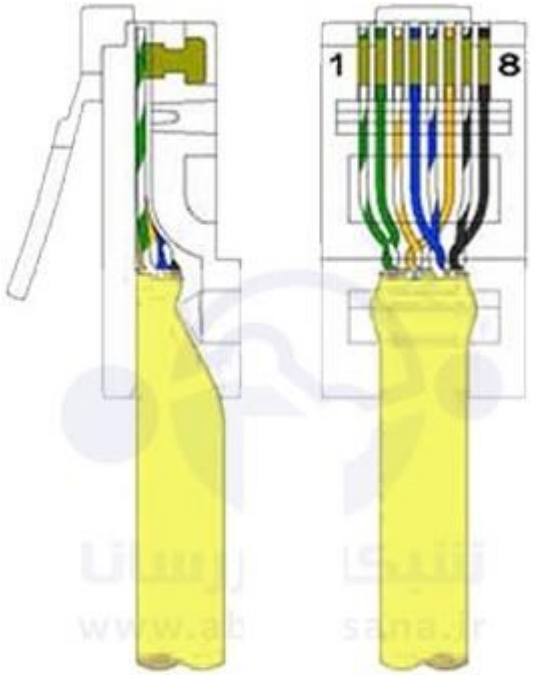
UTP Category:

Cat1:	1Mbps		0.4MHz
Cat2:	4Mbps		4MHz
Cat3:	10Mbps		16MHz
Cat4:	16Mbps		20MHz
Cat5:	100Mbps		100MHz
Cat5e:	1Gbps		100MHz
Cat6:	10Gbps		250MHz
Cat6a:	10Gbps		500MHz
Cat7:	10Gbps		600MHz

TWISTED PAIR ❖

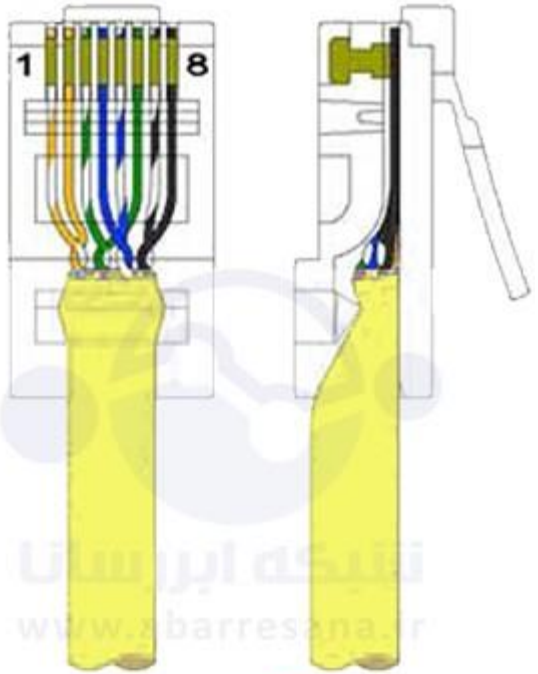


استاندارد و رنگ بندی کابل شبکه:



T-568A

۱	سفید سبز
۲	سبز
۳	سفید نارنجی
۴	آبی
۵	سفید آبی
۶	نارنجی
۷	سفید قهوه ای
۸	قهوه ای

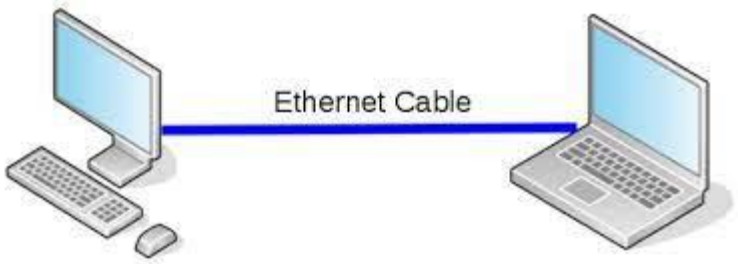


T-568B

۱	سفید نارنجی
۲	نارنجی
۳	سفید سبز
۴	آبی
۵	سفید آبی
۶	سبز
۷	سفید قهوه ای
۸	قهوه ای

استاندارد و رنگ بندی کابل شبکه:

- کابل مستقیم (Straight)



- کابل ضربدری (Crossover)

ابزار شبکه جهت ساخت کابل :

- آچار پرس(سوکت زن)

ابزار شبکه جهت ساخت کابل :

- استریپر

ابزار شبکه جهت ساخت کابل :

- آچارکروز (پانچ)

ابزار شبکه جهت ساخت کابل :

- کف چین

تجهیزات شبکه :

- Patchcord

تجهیزات شبکه :

- Patch pannel
  - UnLoaded

  - Loaded

تجهیزات شبکه :

- Switch
  - Manage
  - UnManage

تجهیزات شبکه :

- MODEM

تجهیزات شبکه :

- Access Point

تجهیزات شبکه :

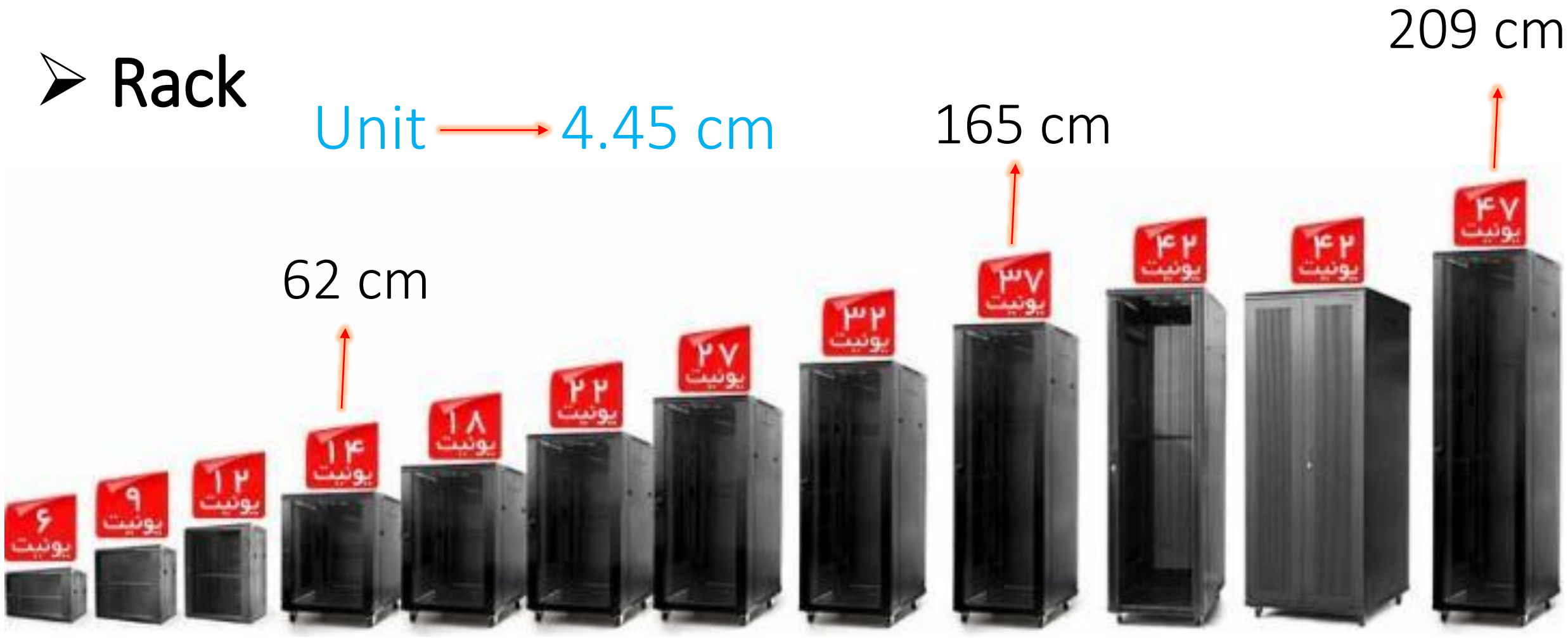
- Router

تجهیزات شبکه :

- Rack
  - رک ایستاده
  - رک دیواری

تجهیزات شبکه :

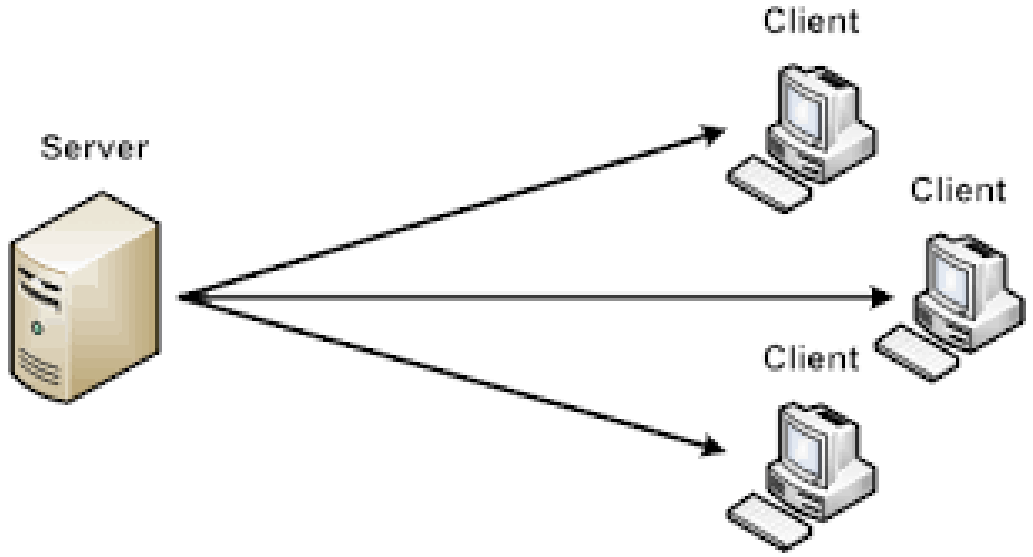
- Rack



نرم افزار شبکه:

Client/Server:

- Client ⟵ سرویس گیرنده خدمات
- Server ⟵ سرویس دهنده خدمات



مزایا و معایب:

- مدیریت متمرکز و راحت
- با خرابی سرور کل شبکه از کار می افتد

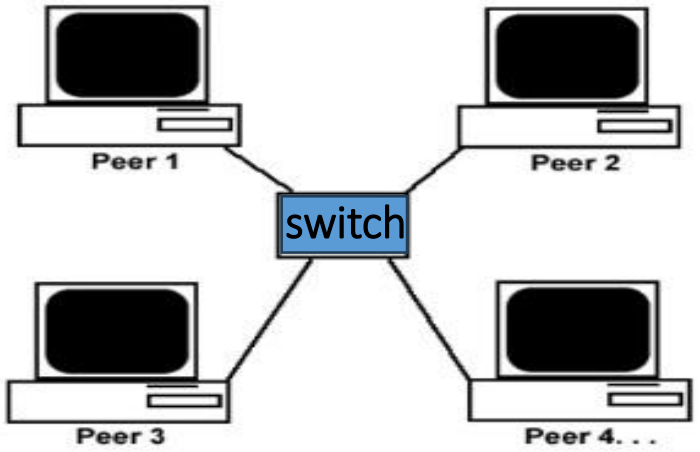
نرم افزار شبکه:

Peer To Peer:

- ✓ سیستم ها هم سرویس گیرنده و هم سرویس دهنده خدمات هستند

مزایا و معایب:

- مناسب برای شبکه های کوچک
- مدیریت غیر متمرکز



P2P Network

اینترنت،اینترانت،اکسترانت:

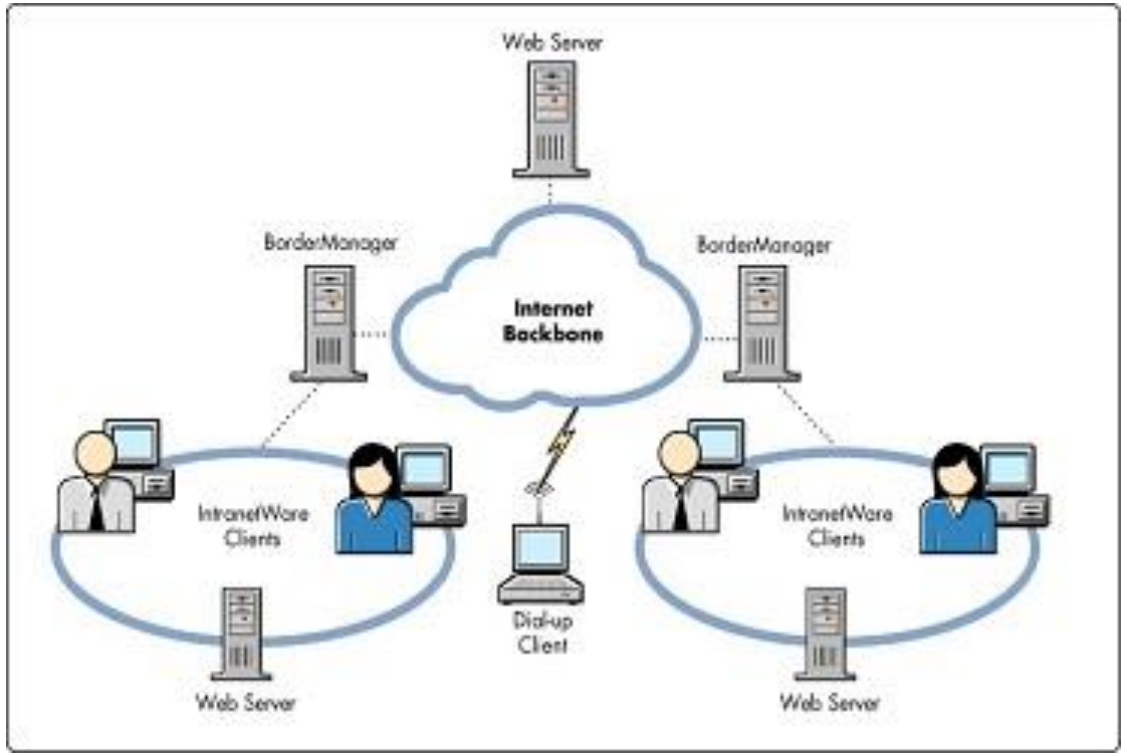
Internet:

- ✓ شبکه‌ای است که به وسیله دستگاه اتصال به شبکه، برای همه قابل دسترسی است.

اینترنت،اینترانت،اکسترانت:

Intranet:

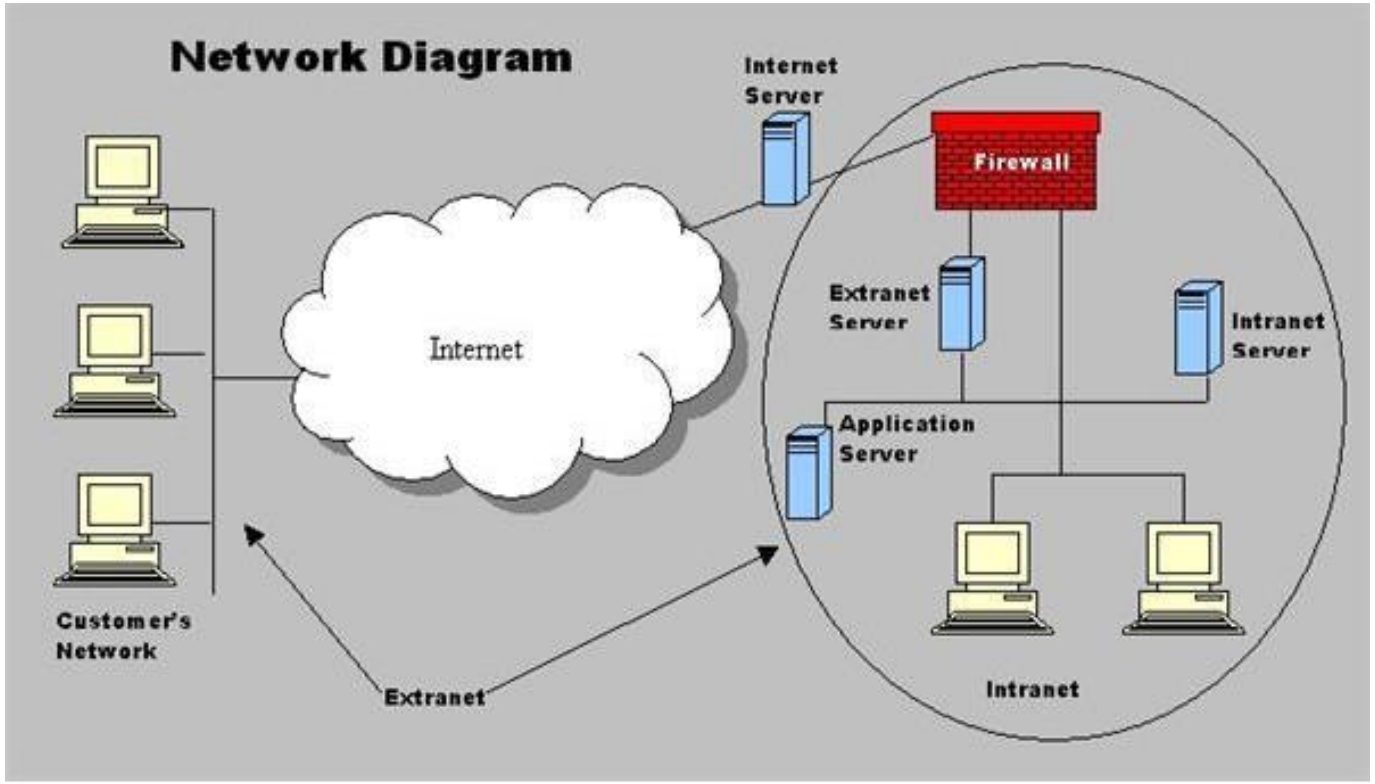
- ✓ شبکه اینترانت برای گروه کوچکی در یک مکان متمرکز،طراحی شده و قابل دسترسی است.



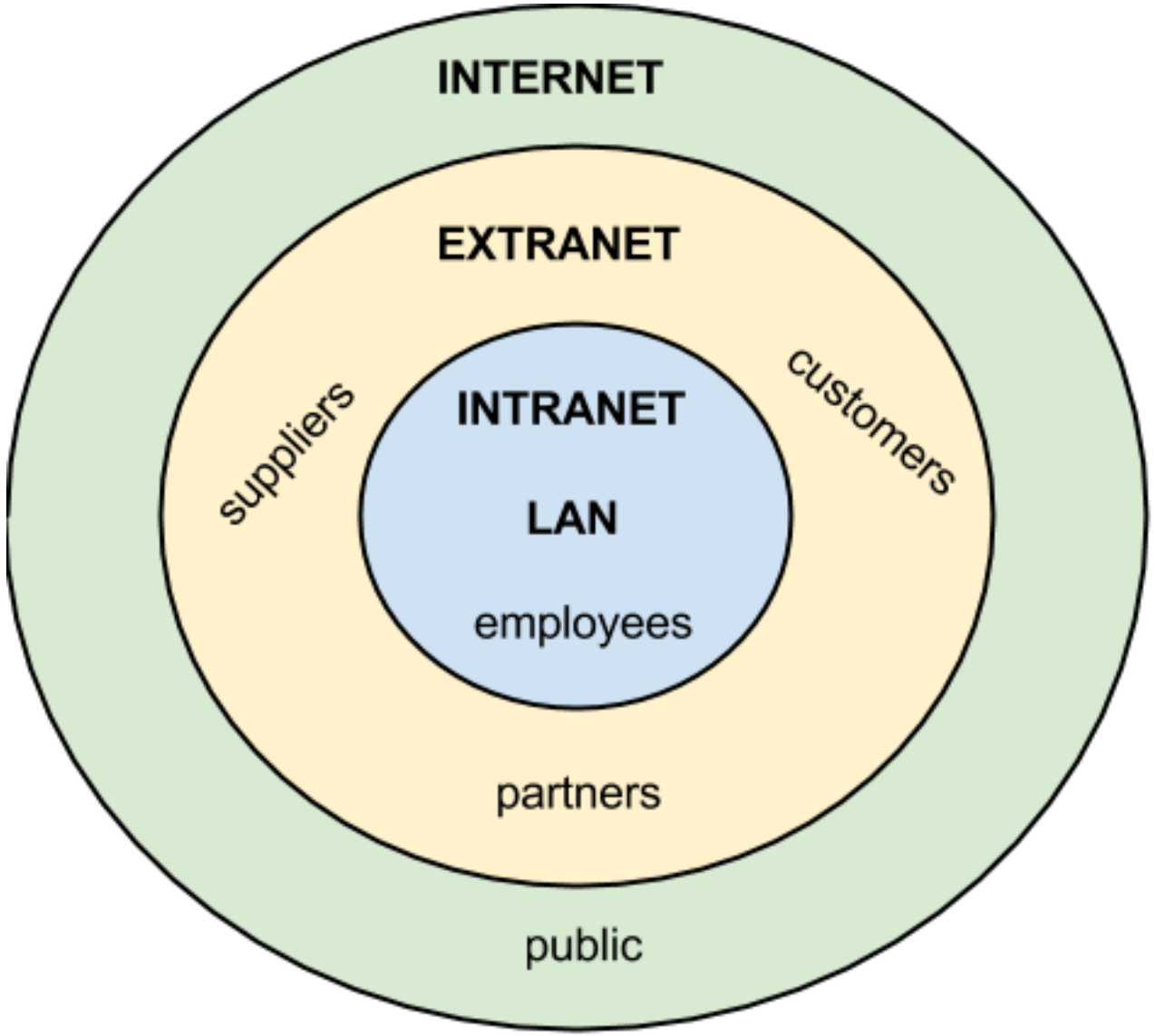
اینترنت،اینترانت،اکسترانت:

Extranet:

- ✓ شبکه اکسترانت برای گروه کوچکی خارج ازیک مکان متمرکز،طراحی شده و قابل دسترسی است.



اینترنت،اینترانت،اکسترانت:



مقیاس شبکه های کامپیوتری :

- (Local Area Network) LAN

شبکه محلی است که محدوده جغرافیایی کوچکی دارد ← خانه ، یک دفتر ،کارخانه

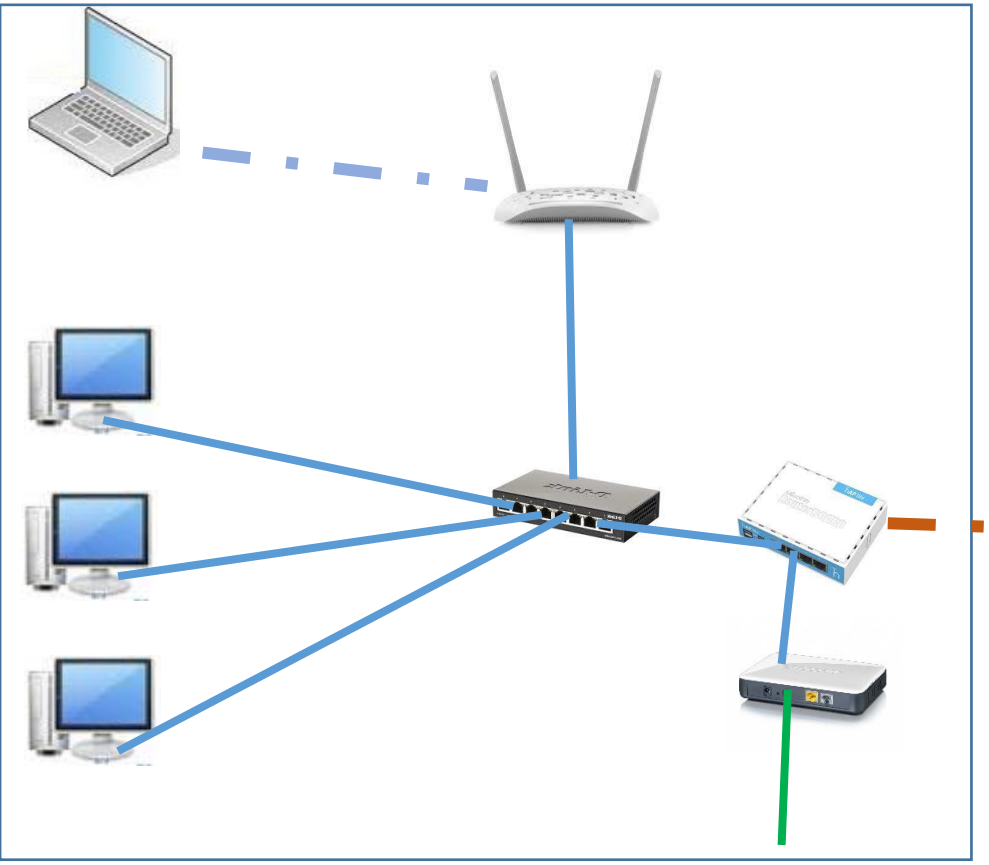
- (Wide Area Network) WAN

شبکه گسترده ای است که ناحیه جغرافیایی وسیعی را پوشش میدهد ← اینترنت

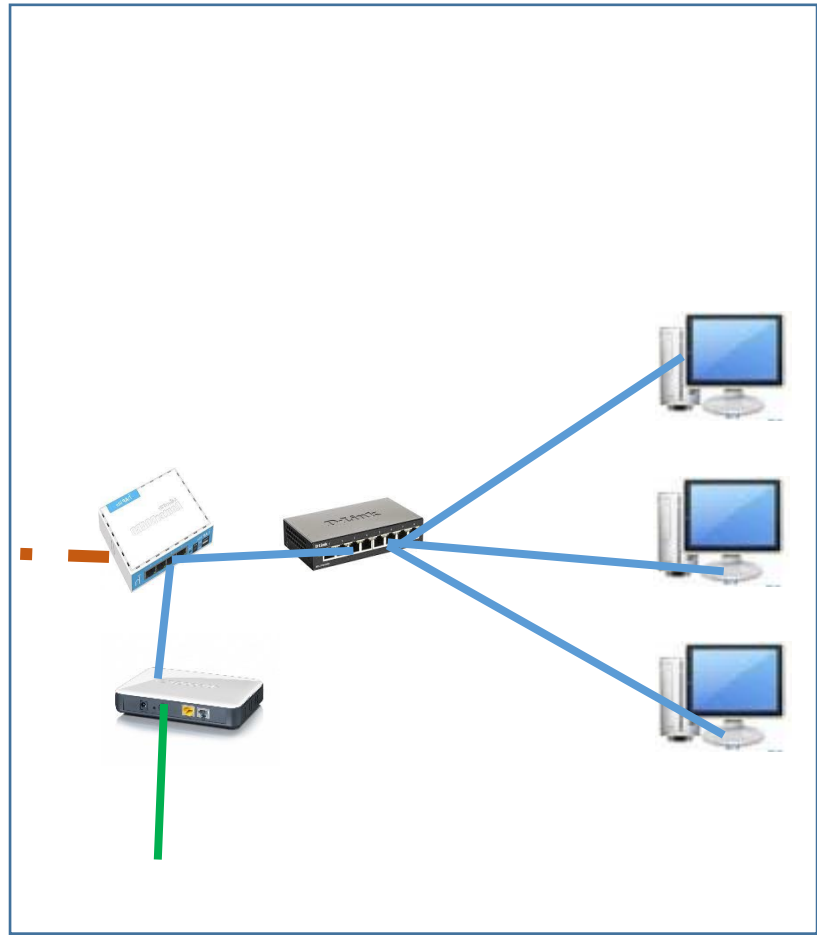
مقیاس شبکه های کامپیوتری :

دفتر اصفهان

دفتر تهران



اینترنت



مدل مرجع OSI:

- ✓ گسترش و عمومیت شبکه ها
- ✓ سخت افزار ها و نرم افزار های متفاوت

به وجود آمدن نوعی ناسازگاری در ارتباط و انتقال داده ها در شبکه های مختلف

Open System Interconnection

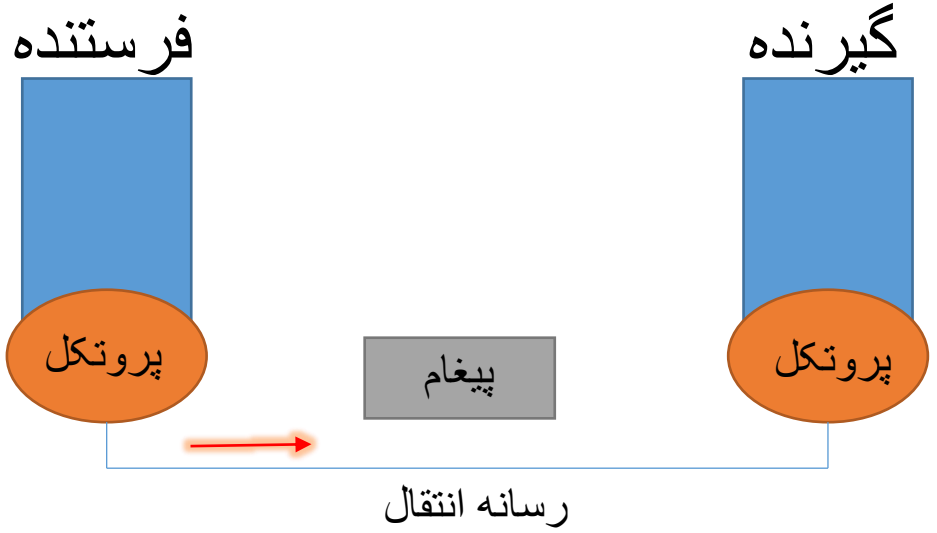
شامل مجموعه ای از استانداردهای ارتباطی شبکه

تا کمپانی های متفاوت بر اساس این مدل، سخت افزار و نرم افزارهای شبکه را طراحی و پیاده سازی کنند

مدل مرجع OSI:

سیستم انتقال داده و اجزای آن:

- **پیغام:** اطلاعاتی که قرار است مبادله شود
- **فرستنده:** دستگاهی که پیغام را ارسال میکند
- **گیرنده:** دستگاهی که پیغام را دریافت میکند
- **رسانه انتقال:** مسیر فیزیکی که پیغام از طریق آن ارسال می شود
- **پروتکل:** مجموعه قواعد و قوانینی که قالب و چگونگی انتقال داده را مشخص می کند



مدل مرجع OSI:

از مفاهیم اصلی شبکه های کامپیوتری:

- **لایه:** به منظور تفکیک وظایف و عملیات لازم جهت انتقال داده
- **معماری شبکه:** مجموعه لایه ها و پروتکلهای پیاده سازی شده در هر لایه
- **آدرس:** شامل آدرس کامپیوتر مبدا، آدرس کامپیوتر مقصد و...

- مدل OSI وظایف و توابع شبکه که در هر لایه انجام می شود را مشخص می کند.
- جداسازی وظایف و توابع شبکه را لایه سازی (Layering) می گویند.

مدل مرجع OSI:

مزایای لایه ها در تقسیم وظایف شبکه

۱-تقسیم شبکه ارتباطی به اجزا کوچکتر و ساده

۲-تعریف واسطه ها و اجزا یک شبکه استاندارد برای توسعه و گسترش در کمپانی های مختلف

۳-مرتبط شدن سخت افزارها و نرم افزارهای مختلف با یکدیگر

۴-عدم تاثیرگذاری تغییرات در یک لایه بر لایه های دیگر

۵-ساده تر شدن فهم یک شبکه با تقسیم آن به اجزا کوچکتر

❖ تمامی این عملیات و روال ها، در **هفت لایه** مدل OSI صورت میگیرد

فرستنده

7

6

5

4

3

2

1

رسانه انتقال

گیرنده

7

6

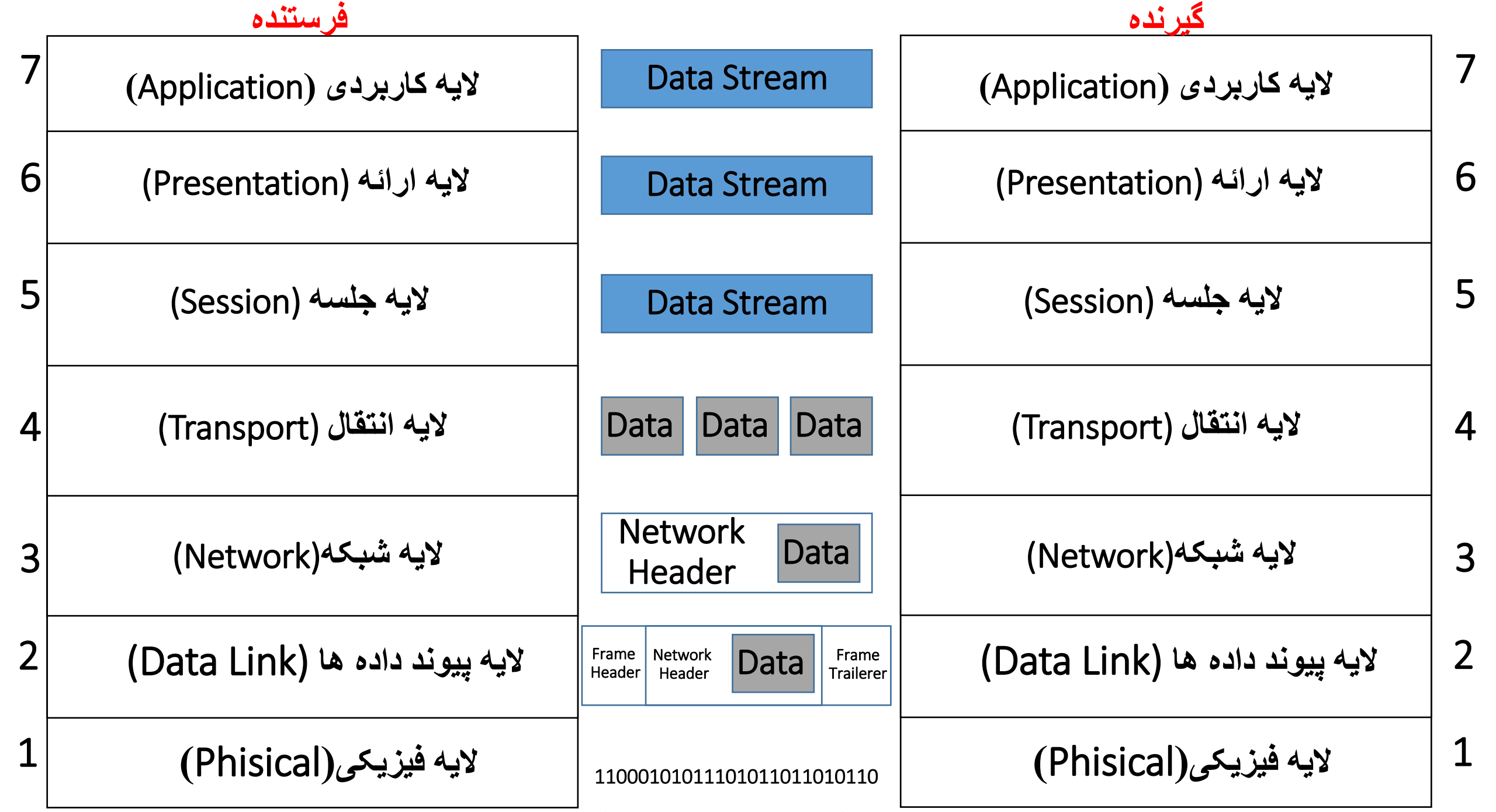
5

4

3

2

1


فرستنده
گیرنده
7
لایه کاربردی (Application)
Data Stream
لایه کاربردی (Application)
7
6
لایه ارائه (Presentation)
Data Stream
لایه ارائه (Presentation)
6
5
لایه جلسه (Session)
Data Stream
لایه جلسه (Session)
5
4
لایه انتقال (Transport)
Data
Data
Data
لایه انتقال (Transport)
4
3
لایه شبکه(Network)
Network Header
Data
لایه شبکه(Network)
3
2
لایه پیوند داده ها (Data Link)
Frame Header
Network Header
Data
Frame Trailerer
لایه پیوند داده ها (Data Link)
2
1
لایه فیزیکی(Phisical)
11000101011101011011010110
لایه فیزیکی(Phisical)
1

مدل مرجع OSI:

7

لایه کاربردی
(Application)

- نزدیک ترین لایه به کاربر
- فراهم کردن سرویس های شبکه ای لازم برای برنامه های کاربردی و کاربران

- برنامه های مرورگر وب
- برنامه های پست الکترونیکی
- برنامه های انتقال فایل
- Telnet

مدل مرجع OSI:

6

لایه ارائه (Presentation)

- تبدیل کدهای مختلف داده دریافتی گیرنده
- رمزگذاری داده در سمت فرستنده و رمز گشایی در سمت گیرنده
- فشرده سازی داده و از حالت فشرده خارج کردن داده

❖ **اطلاعاتی را که از لایه کاربردی فرستنده ارسال میشود برای لایه کاربردی گیرنده قابل فهم می کند.**

مدل مرجع OSI:

5

لایه جلسه
(Session)

- ایجاد،مدیریت و اتمام جلسات بین دو کامپیوتر
- تصدیق هویت فرستنده
- اعتبار سنجی پیغام ها
- همزمان سازی تبادل داده بین فرستنده و گیرنده با قرار دادن نقاط وارسی

❖ **در صورت قطع ارتباط و ارتباط مجدد بین فرستنده و گیرنده، انتقال داده از زمان قطع ارتباط دوباره انجام میگیرد.**

مدل مرجع OSI:

4

لایه انتقال (Transport)

- تحویل داده به صورت مطمئن با کشف خطای انتقال
- کنترل جریان داده
- ایجاد ،نگهداری و حذف مدار منطقی برای انتقال داده
- شکستن و قطعه قطعه کردن اطلاعات و شماره گذاری آنها

❖ ارائه کیفیت خدمات (Quality Of Service)

مدل مرجع OSI:

3

لایه شبکه
(Network)

- آدرس دهی منطقی ← IP Address
- کنترل ازدحام و ترافیک داده
- مسیریابی بین کامپیوترهای فرستنده و گیرنده درون شبکه
- تحویل داده به گیرنده به صورت نامطمئن

❖ تحویل مطمئن داده ، به لایه های بالاتر (انتقال) سپرده می شود.

مدل مرجع OSI:

2

لایه پیوند داده ها
(Data Link)

- آدرس دهی فیزیکی ← MAC Address
- تعیین نحوه دسترسی به رسانه انتقال و مدیریت کانال
- تحویل مرتب بسته های داده
- کنترل خطا و خطایابی داده های منتقل شده
- کنترل جریان داده بین فرستنده و گیرنده

❖ کنترل کننده لایه فیزیکی می باشد و برای لایه فیزیکی مشخص میکند که چه کاری را باید انجام دهد

مدل مرجع OSI:

1
لایه فیزیکی (Phisical)

- مبادله داده به صورت تعدادی بیت بر روی رسانه انتقال بدون توجه به نوع و محتوای داده
- بیان مشخصات لایه فیزیکی بین کامپیوترها نظیر :
  - مشخصات فیزیکی
  - نوع سیگنالهای انتقال
  - نوع رسانه انتقال

❖ این لایه صرفا سخت افزاری است.

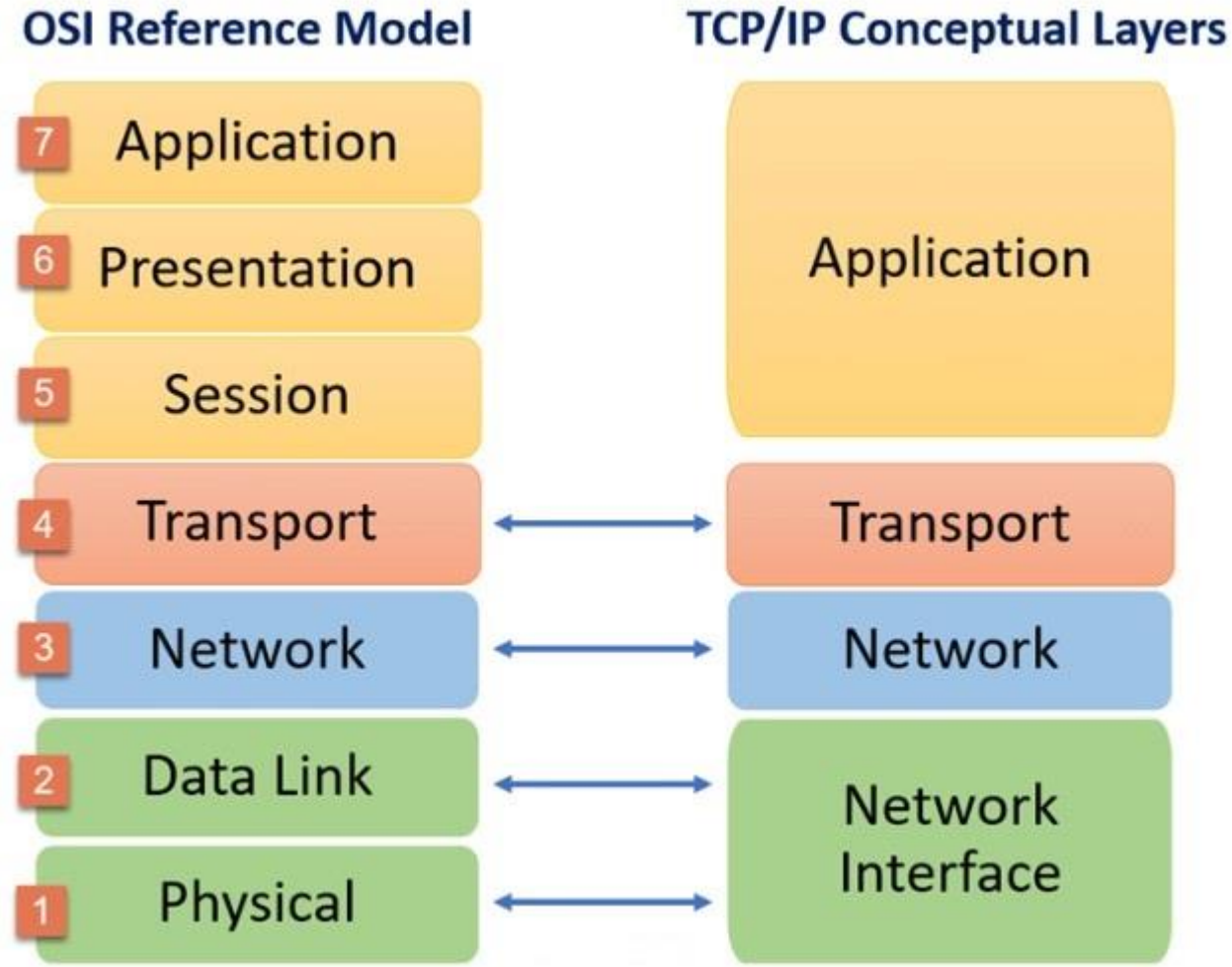
پروتکل(Protocol):

زبان مشترک کامپیوترها جهت ارتباط با یکدیگر

پروتکل های استاندارد:

- **NET BEUI**
- **IPX/SPX**
- **Apple Talk**
- **TCP/IP**

Transmission Control Protocol / Internet Protocol :TCP/IP

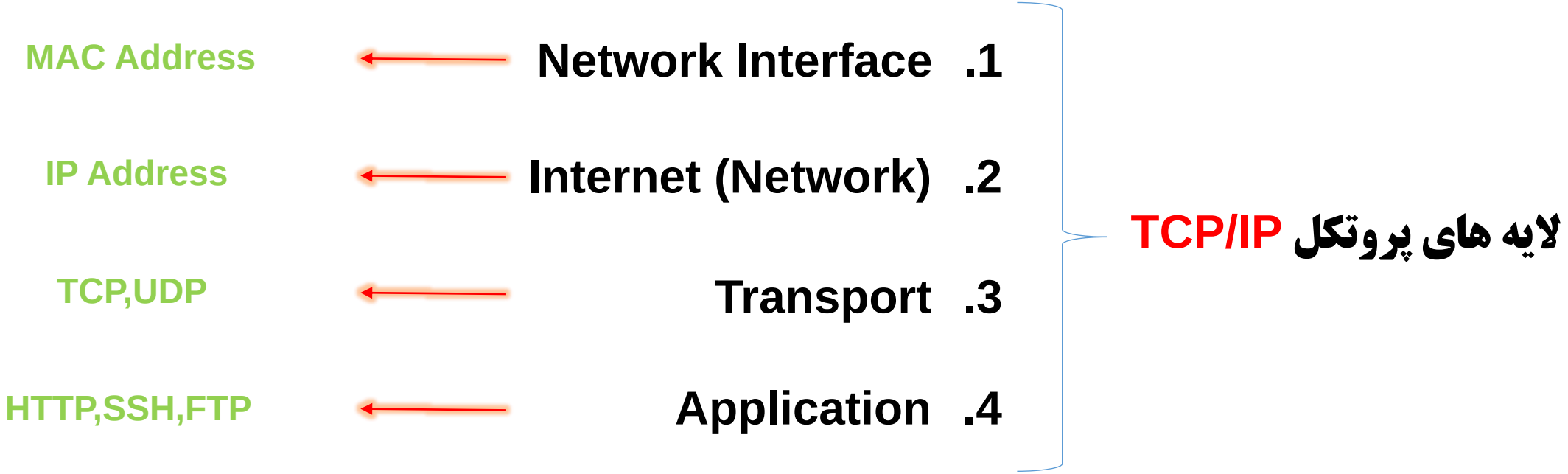


TCP/IP: Transmission Control Protocol / Internet Protocol

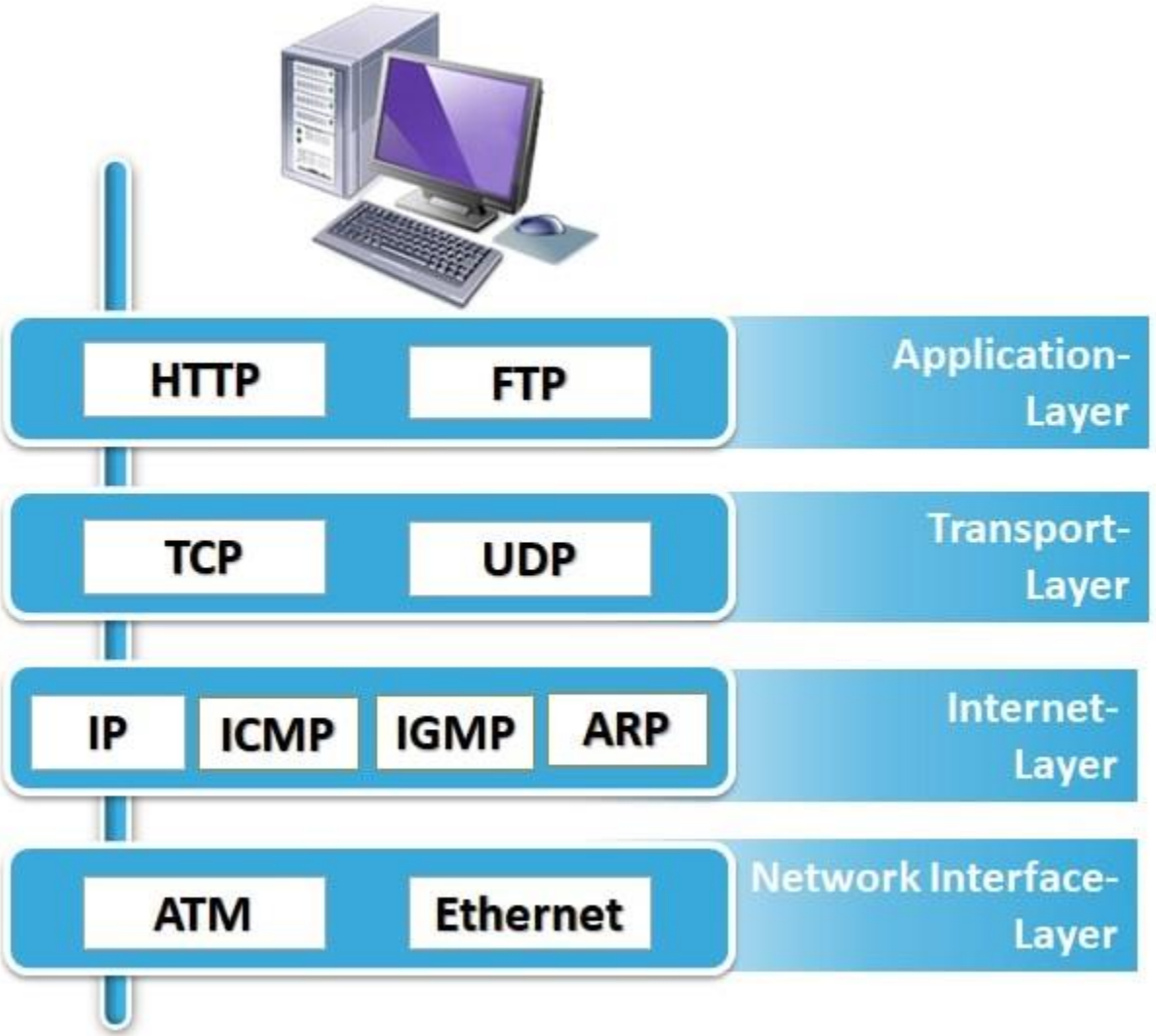
Transmission Control Protocol (پروتکل کنترل انتقال) ← چگونگی تبادل اطلاعات بین دو کامپیوتر

Internet Protocol (پروتکل اینترنت) ← چگونگی برقراری ارتباط بین دو کامپیوتر

پروتکل TCP/IP



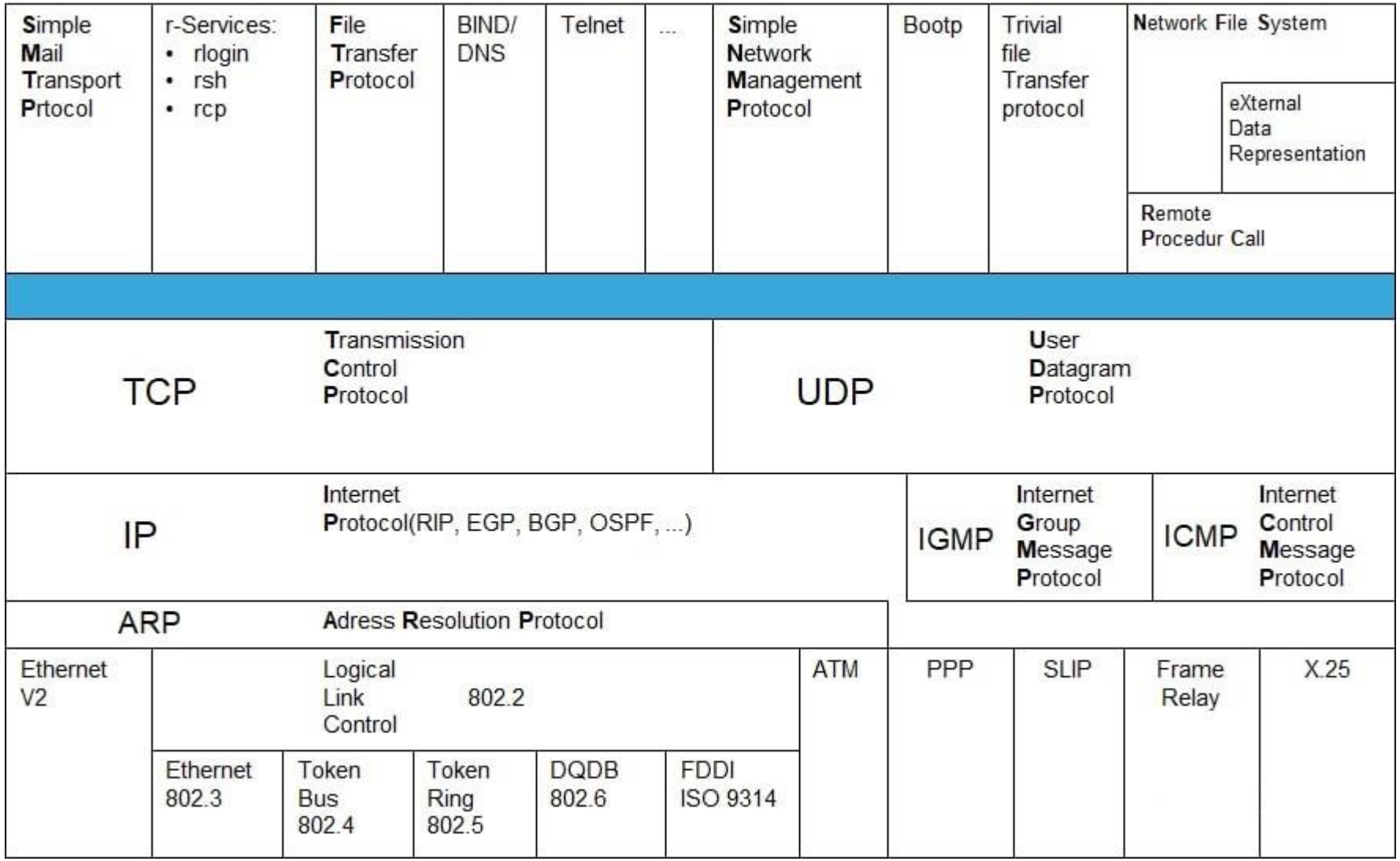
پروتکل TCP/IP



ویژگی های TCP/IP

- امنیت بالا
- توسعه پذیری
- سازگاری با محیطهای مختلف

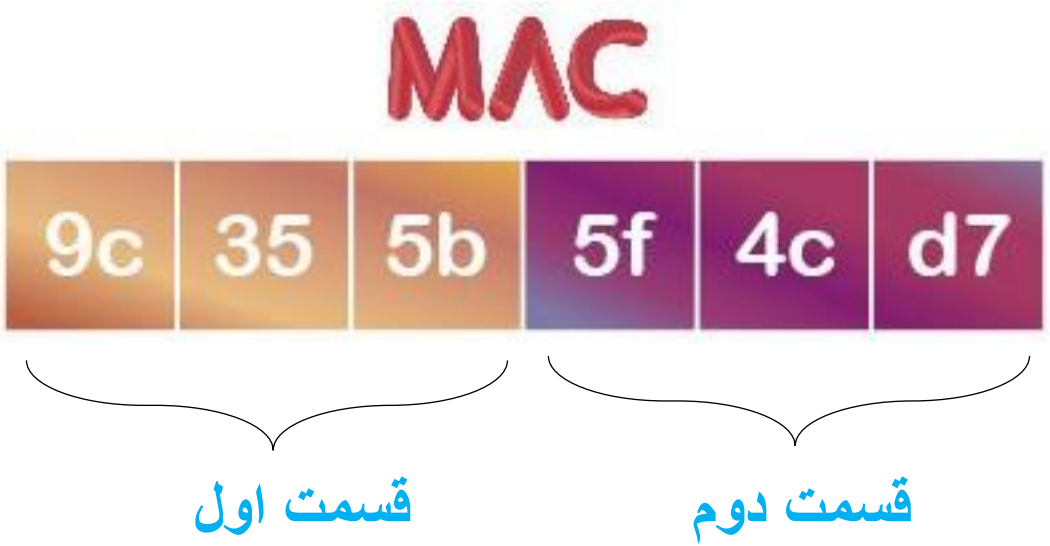
پروتکل TCP/IP



MAC Address

به آدرس فیزیکی دستگاه، کنترل دسترسی رسانه (media access control) یا به اختصار MAC می‌گویند

جهت شناسایی دستگاه ومتمایز کردن آن از میلیون‌ها دستگاه دیگر



قسمت اول:

توسط شرکت سازنده کارت شبکه تعیین میشود

قسمت دوم:

تعداد دستگاههای قابل شماره گذاری برای آن شرکت

IP Address

جهت ارتباط دو سیستم در یک شبکه به یک آدرس منطقی نیاز است

- IP Version 4 ← 192.168.1.10
- IP Version 6 ← 2702:A0B3:8012:D0E5:0000:0000:0000:B25F

IP Address

- IP Version 4 ← 32 bit

✓ bit: کوچکترین واحد اندازه گیری در کامپیوتر که یا صفر است یا یک

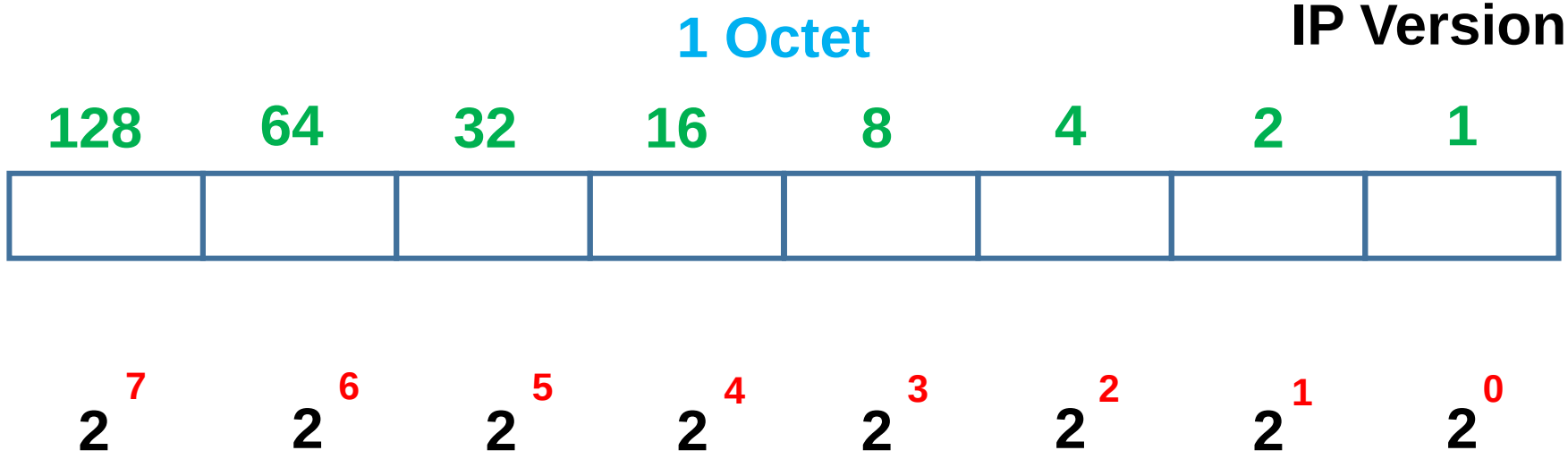
32 bit = 4 *(8 bit)

8 bit = 1 Byte = 1 Octet

Dotted Decimal Notation	10	1	2	3
Binary Bits	00001010	00000001	00000010	00000011
	Octet 1	Octet 2	Octet 3	Octet 4

IP Address

- IP Version 4



IP Address

- IP Version 4

1 Octet

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1

255 ⬅======

IP Address

- IP Version 4

1 Octet

128	64	32	16	8	4	2	1
0	1	1	0	0	1	0	1

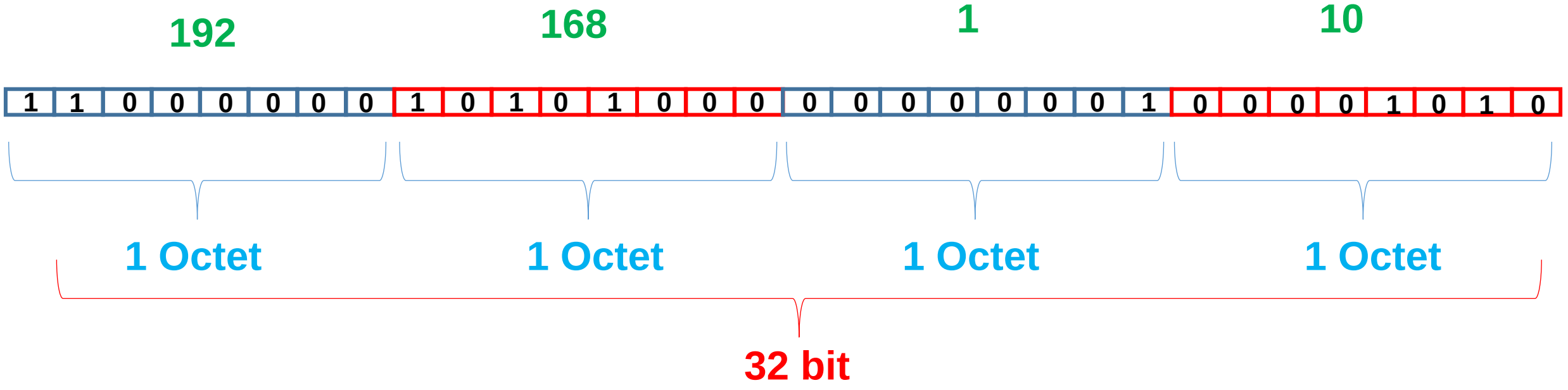
2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

0 + 64 + 32 + 0 + 0 + 4 + 0 + 1

101 ⬅======

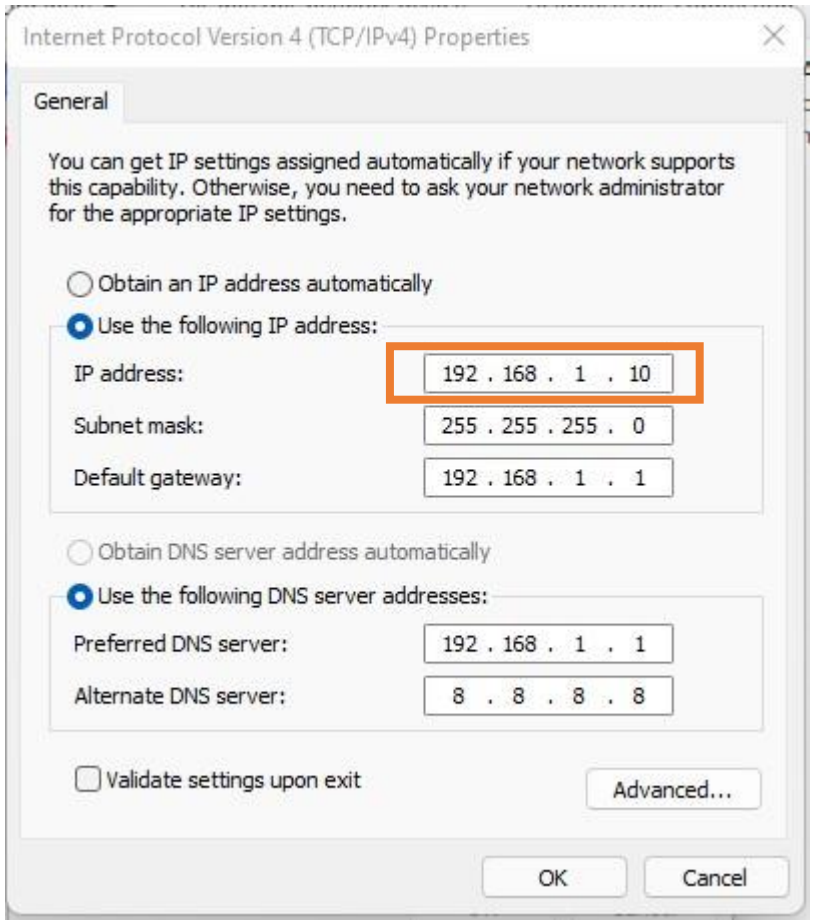
IP Address

- IP Version 4



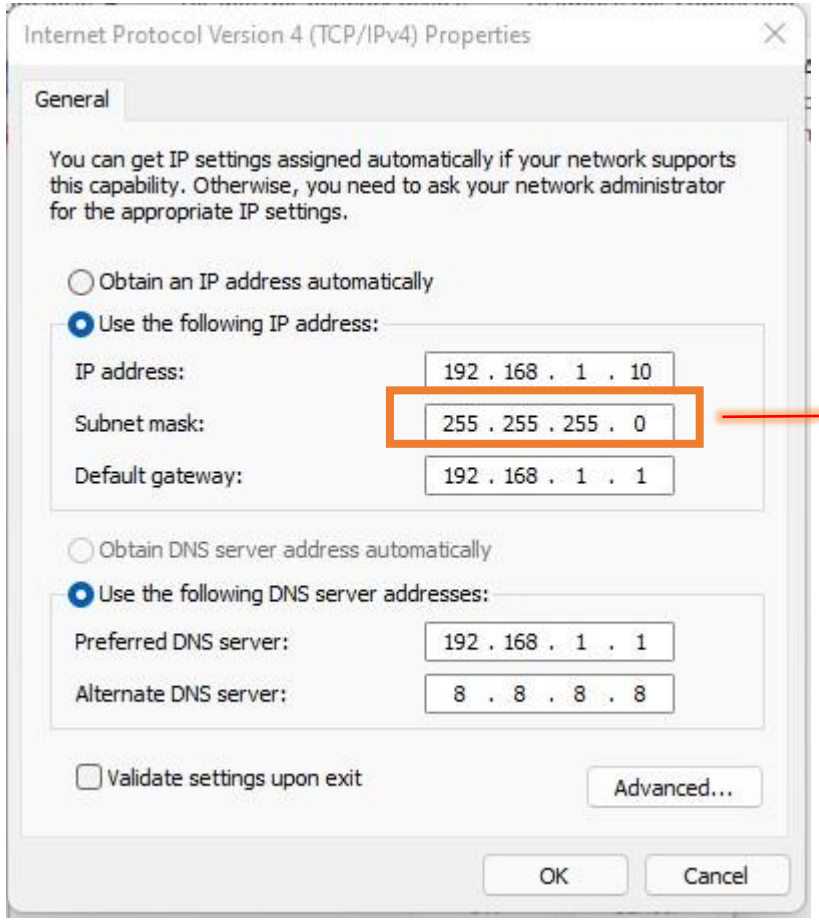
IP Address

- IP Version 4



Subnet mask

- IP Version 4

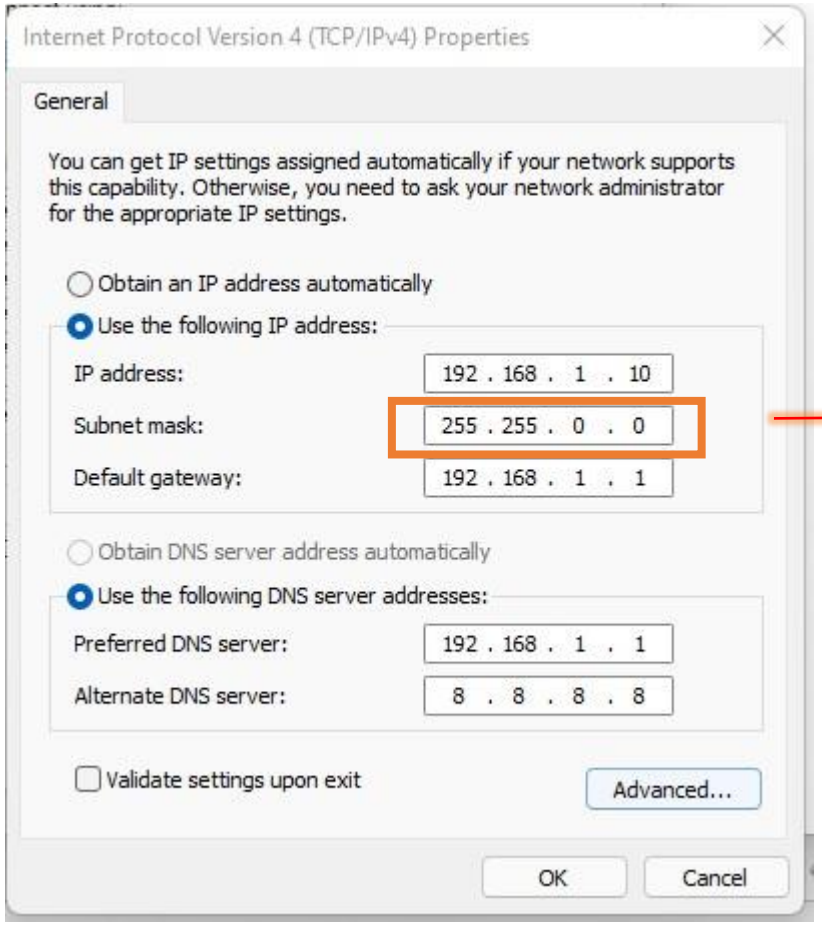


❖ تعداد IP قابل استفاده:

255

Subnet mask

- IP Version 4



❖ تعداد IP قابل استفاده:

255 * 255

65,025

Subnet mask

- IP Version 4

- NetId (Network Identifier): شماره شبکه
- HostId (Host Identifier): شماره کامپیوتر

Dotted Decimal Notation	10	1	2	3
IP Address (in Binary)	00001010	00000001	00000010	00000011
Subnet Mask	11111111	00000000	00000000	00000000

Network Bits | Host Bits

Subnet mask

- IP Version 4

✓ قانون تفکیک دو بخش Netid و HostId کلاس بندی است

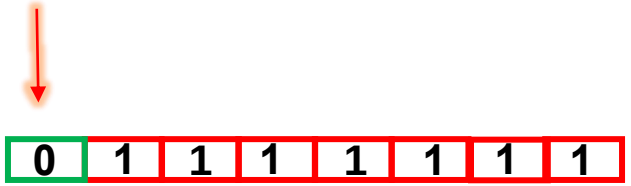
✓ با کلاس بندی می توان شبکه هایی با سایزهای مختلف ایجاد کرد

Address Class	Value in First Octet	Classful Mask	Classful Mask
Class A	1-126	255.0.0.0	/8
Class B	128-191	255.255.0.0	/16
Class C	192-223	255.255.255.0	/24
Class D	224-239		
Class E	240-255		

Subnet mask

- IP Version 4

❑ Class A



✓ بیت اول Octet اول همواره صفر است

✓ ۲۴ بیت برای Host Id باقی میماند ← ۲ به توان ۲۴ = 16,777,216

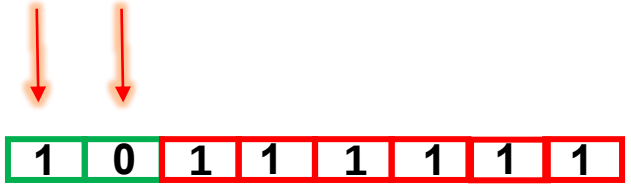
✓ اگر در Net Id تمام بیت ها را یک کنیم (به جز بیت اول که همواره صفر است) به عدد ۱۲۷ میرسیم

Loopback Address: برای تست و سلامتی کارت شبکه مورد استفاده است ← 127.0.0.1

Class A

Network	Host		
1 to 126	x	x	x

Subnet mask



- IP Version 4

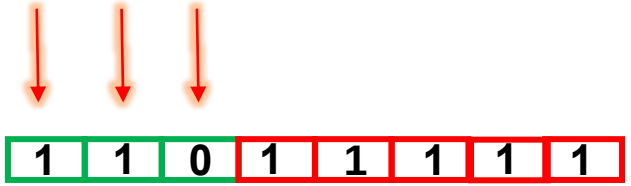
❑ Class B

- ✓ دو تا octet اول شماره شبکه هست و دوتا octet باقی مانده Hostld هستند
- ✓ دو بیت اول Octet اول با ۱۰ شروع می شود
- ✓ در مجموع برای Netid ما از ۱۴ بیت میتوانیم استفاده کنیم
- ✓ ۱۶ بیت برای Host Id باقی می ماند ← ۲ به توان ۱۶ = 65,636

Class B

Network		Host	
128 to 191	x	x	x

Subnet mask



- IP Version 4

Class C ❑

- ✓ سه Octet اول مربوط به NetId یا شماره شبکه می باشد
- ✓ فقط Octet آخر مربوط به HostId می باشد
- ✓ سه بیت اول Octet اول ۱۱۰ می باشد
- ✓ در مجموع برای Netid ما از ۲۱ بیت میتوانیم استفاده کنیم
- ✓ ۸ بیت برای Host Id باقی میماند ← ۲ به توان ۸ = 256

Class C

Network			Host
192 to 223	x	x	x

IP Address

- IP Version 4

➢ Broadcast ⟵ اگر تمام HostId ها برابر با ۱ باشد

192.168.1.255

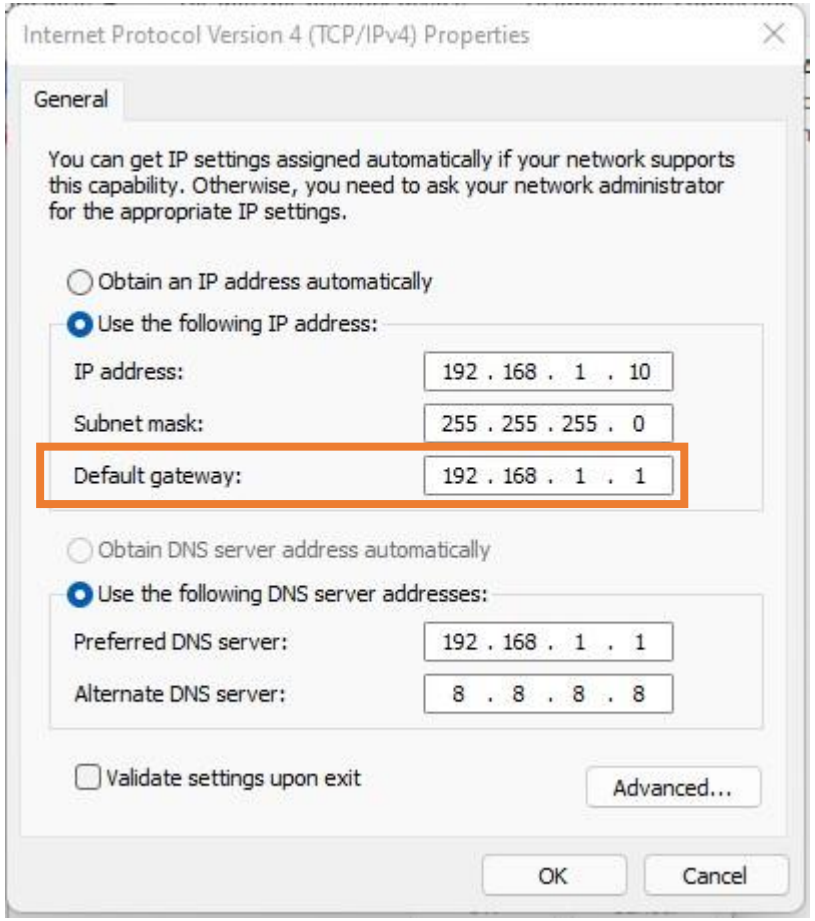
➢ Network Number ⟵ اگر تمام HostId ها برابر با 0 باشد

192.168.1.0

⟵ آدرس ابتدا و انتهایی هر HostID نمیتواند به عنوان آدرس معتبر برای سیستم ها باشند .

192.168.1.1-254

Gateway


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server: 8 . 8 . 8 . 8
Validate settings upon exit
Advanced...
OK
Cancel

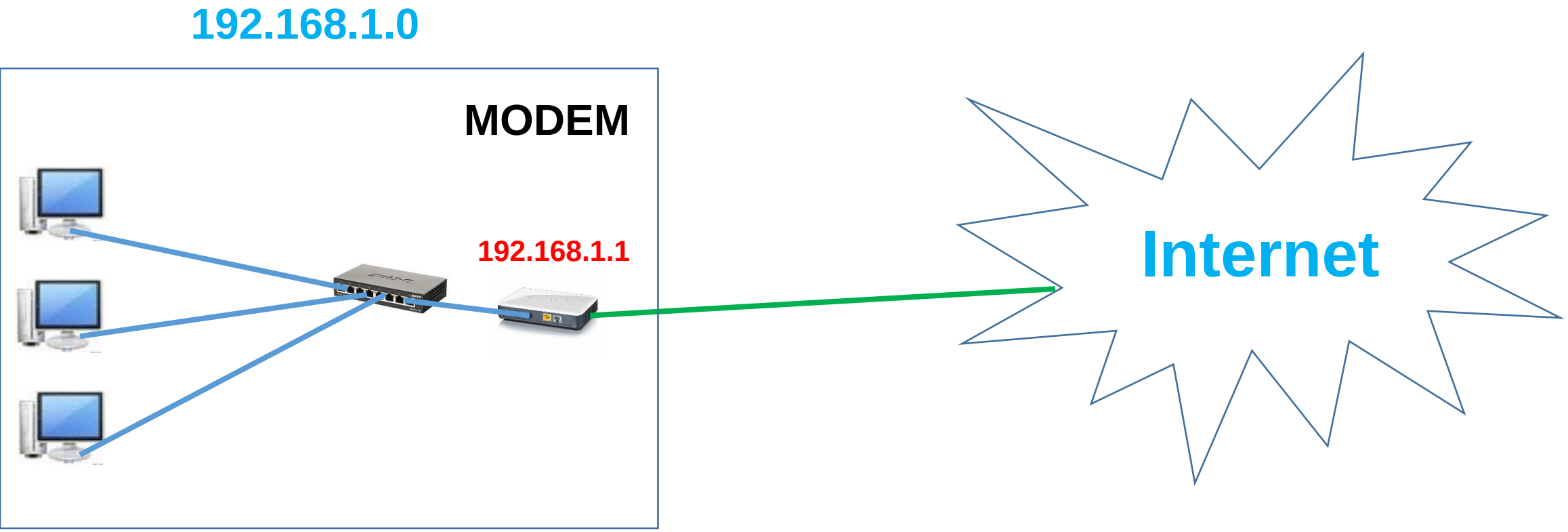
Gateway

✓ دستگاهی که شبکه ما را به اینترنت یا سایر شبکه ها مرتبط میسازد

- Router
- Switch Manage
- MODEM → 192.168.1.1

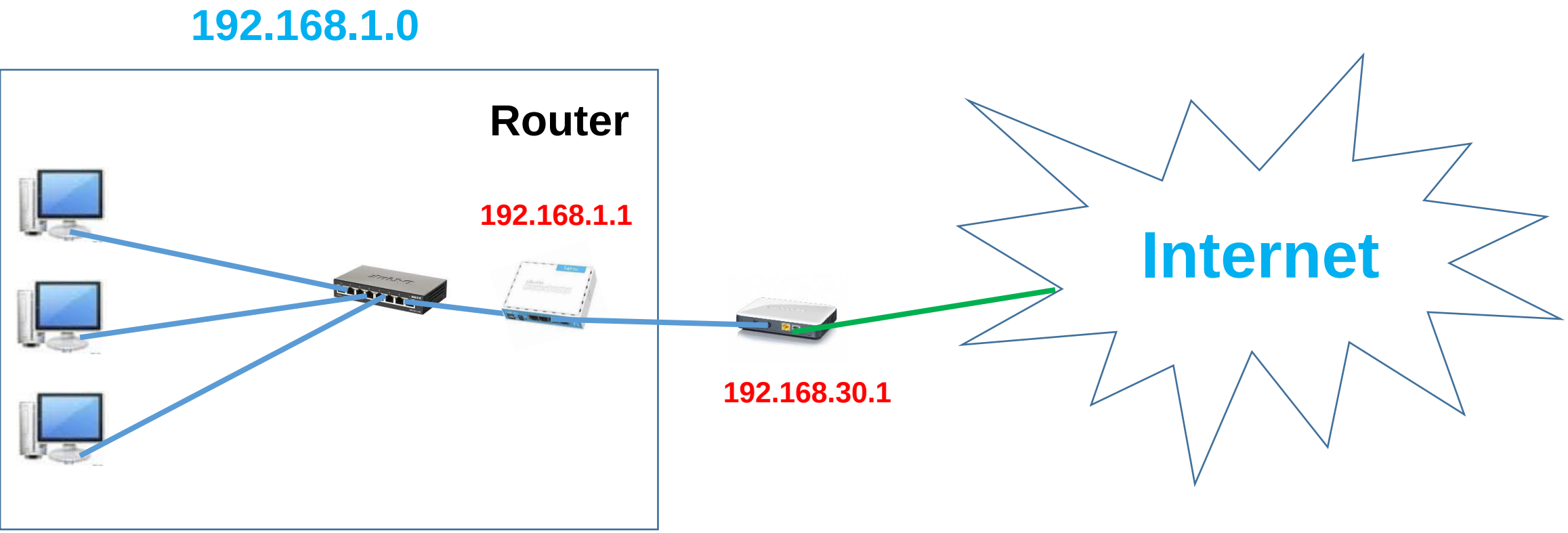
Gateway

✓ دستگاهی که شبکه ما را به اینترنت یا سایر شبکه ها مرتبط میسازد



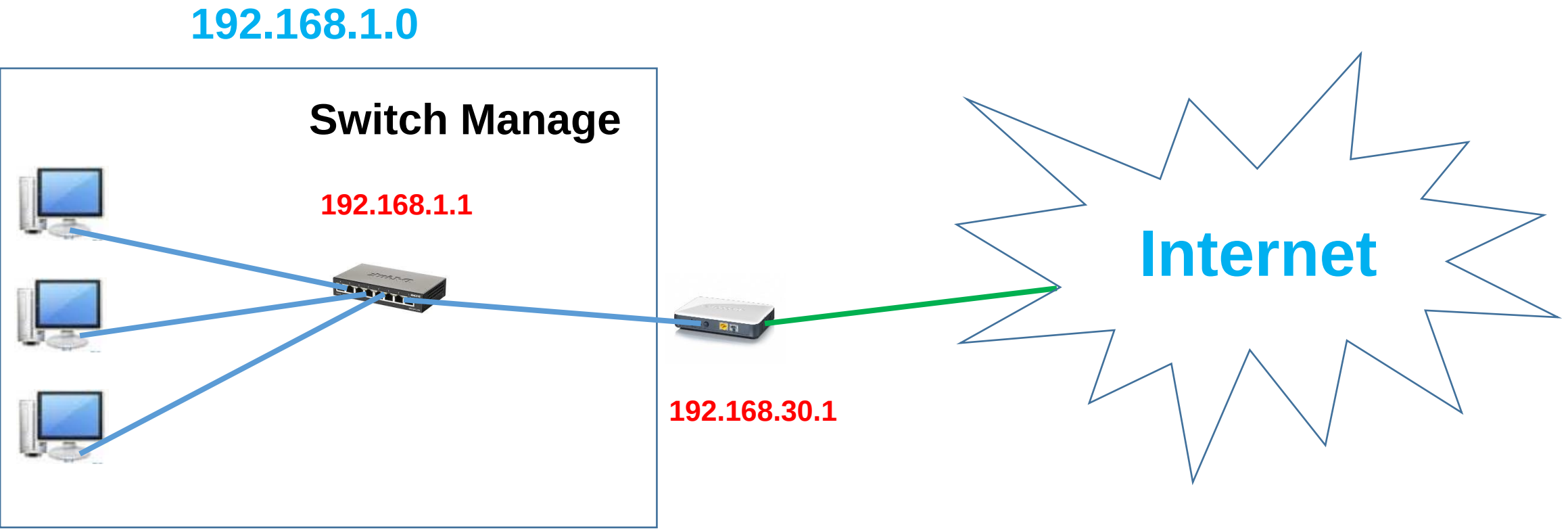
Gateway

✓ دستگاهی که شبکه ما را به اینترنت یا سایر شبکه ها مرتبط میسازد

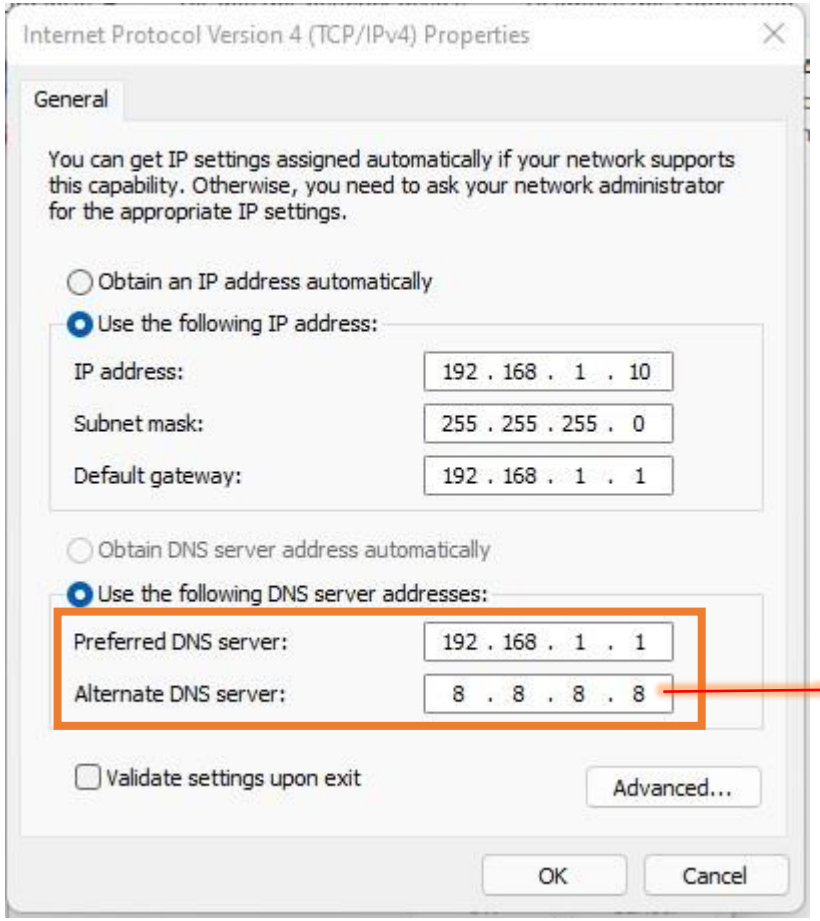


Gateway

✓ دستگاهی که شبکه ما را به اینترنت یا سایر شبکه ها مرتبط میسازد



Domain Name System ← DNS



✓ جهت تبدیل اسم دامنه ها به IP Address و بالعکس

Google DNS

DNS

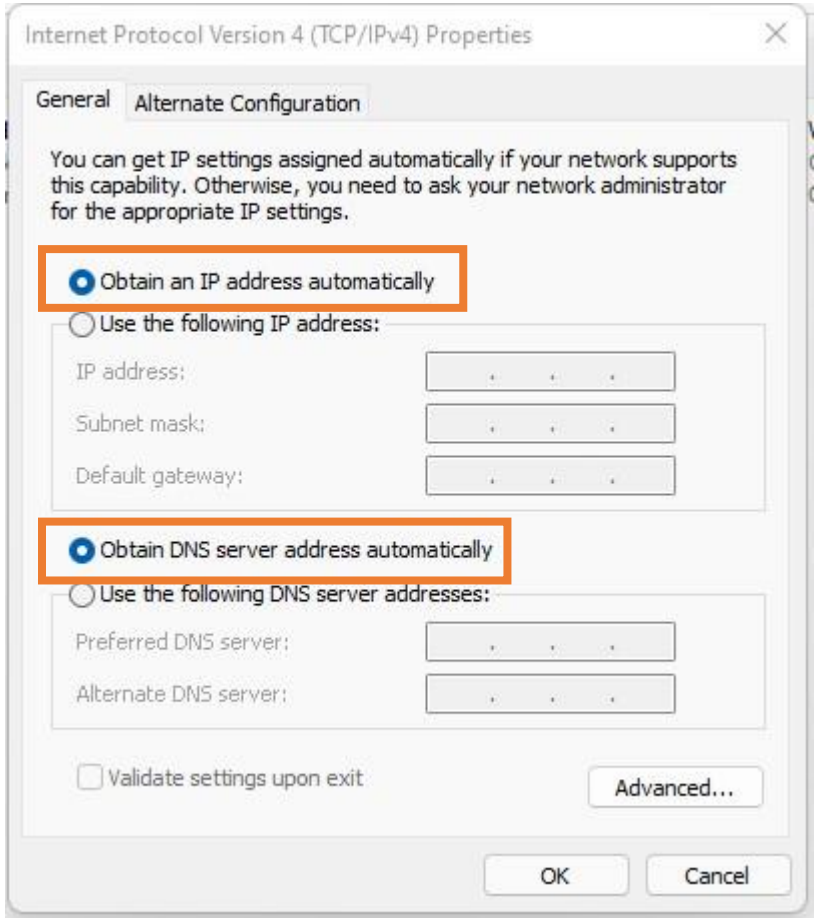
Domain Name System

جهت چک کردن ip یک سایت و دامنه https://dnschecker.org

جهت خرید یک دامنه https://www.nic.ir

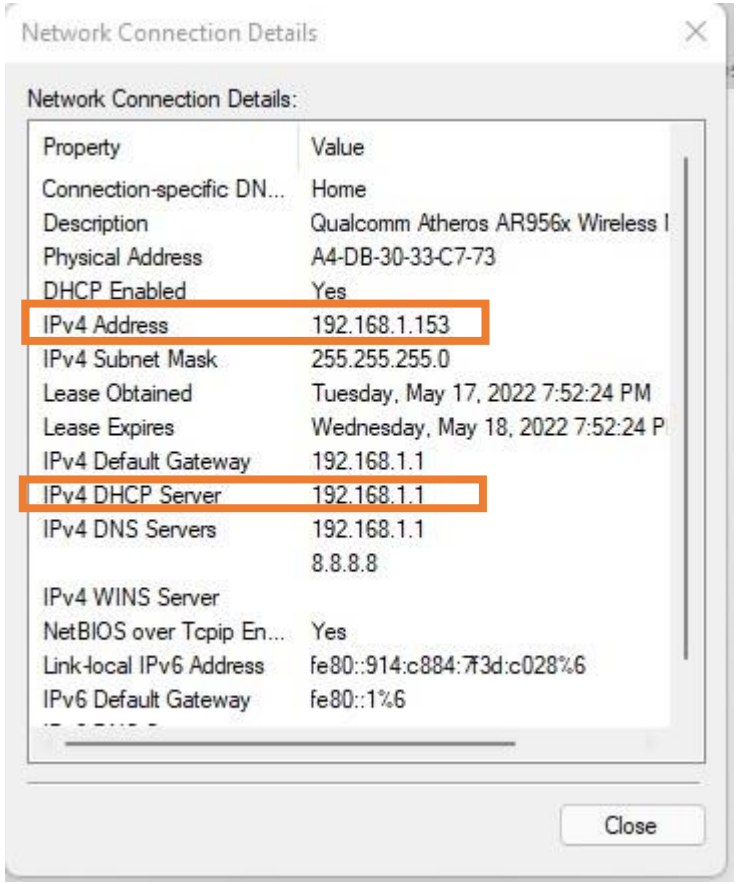
جهت انتساب یک IP به نام یک دامنه https://www.dynu.com

Dynamic Host Configuration Protocol ← DHCP



- ✓ اختصاص دادن آدرس IP به client های شبکه به صورت اتوماتیک

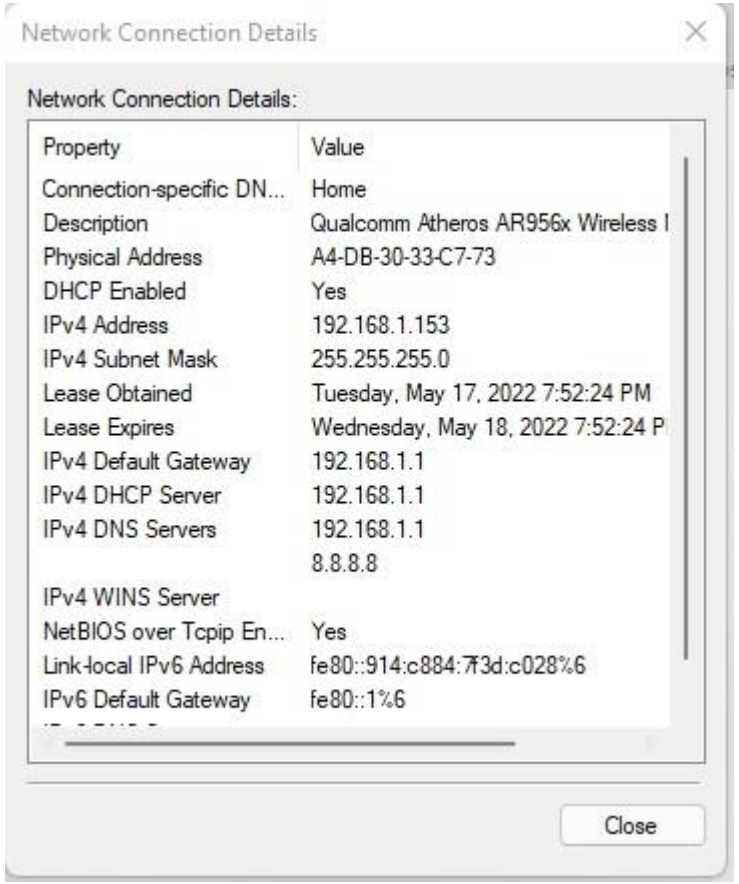
Dynamic Host Configuration Protocol ← DHCP



❑ دلایل استفاده از DHCP

- ✓ تعداد کلاینت های موجود در شبکه زیاد باشند
- ✓ اینکه چه IPهایی مصرف شده و چه IPهایی مصرف نشده است
- ✓ احتمال خطا به صورتی دستی تقریبا زیاد است
- ✓ با استفاده از DHCP کنترل و مدیریت روی IP ها آسان تر است

Dynamic Host Configuration Protocol ← DHCP



❑ مزایای استفاده از DHCP

- ✓ آدرس دهی به صورت سریع انجام میشود
- ✓ پیکربندی امن و قابل اطمینان
- ✓ مدت زمان مدیریت پیکربندی را کاهش میدهد

Port

- Hardware Port
- Software Port

Software Port ❑

- ✓ پورت نرم افزاری بخشی بسیار مهم از یک آدرس اینترنتی می باشد
- ✓ پورت نرم افزاری در تعیین مقصد جهت ارسال و دریافت بسته ها کمک می کنند
- ✓ Portهای نرم افزاری تعیین می کنند که کامپیوترها، اطلاعات را از یک آی پی مشخص با یک پورت مشخص، ارسال و دریافت کنند.

Port

Software Port ❑

Protocol	PORT	Protocol	PORT
HTTP	80	RDP	3389
HTTPS	443	DNS	53
FTP	21	SMTP	587
SSH	22	POP3	995
TELNET	23	SQL	1433

Network Address Translation ← NAT

NAT in MODEM ❑

مودم آدرس‌های داخلی را به آدرس های جهانی که روی شبکه خارجی و اینترنت قابل استفاده هستند، تبدیل می‌کند

192.168.1.1

5.37.201.250

IP: 192.168.1.10

GW: 192.168.1.1

DNS: 192.168.1.1

Command-Line

- ipconfig
- ping
- tracert

Command-Line

- ipconfig
  - /all → مشخصات کامل نتورک سیستم
  - /release → پس دادن آدرس موجود
  - /renew → گرفتن آدرس جدید

Command-Line

- ping

-t → تکرار ممتد (پیش فرض 4 بار)

-n count → تکرار به تعداد مشخص

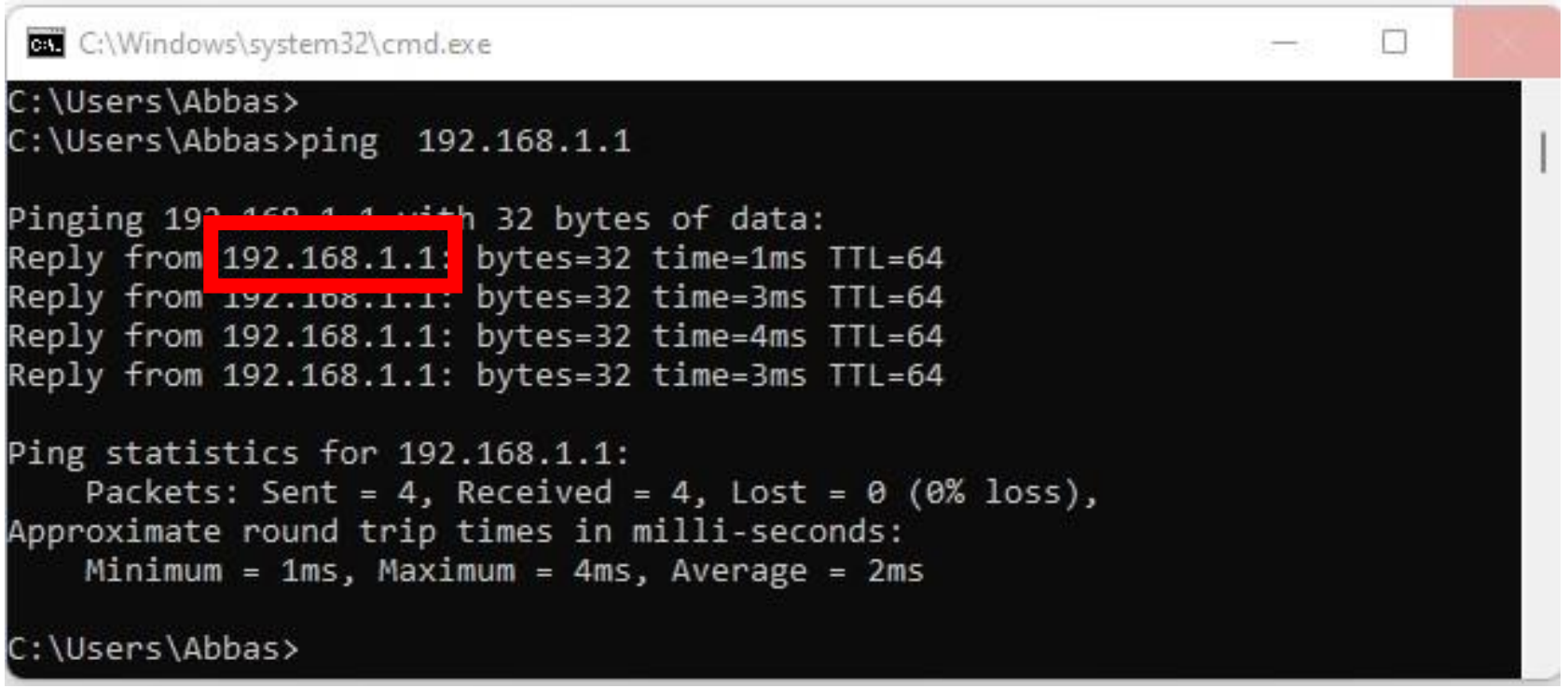
-l size → افزایش حجم پکت ها(پیش فرض 32B)

-a → بدست آوردن نام سیستم مقصد

target-name

- ping

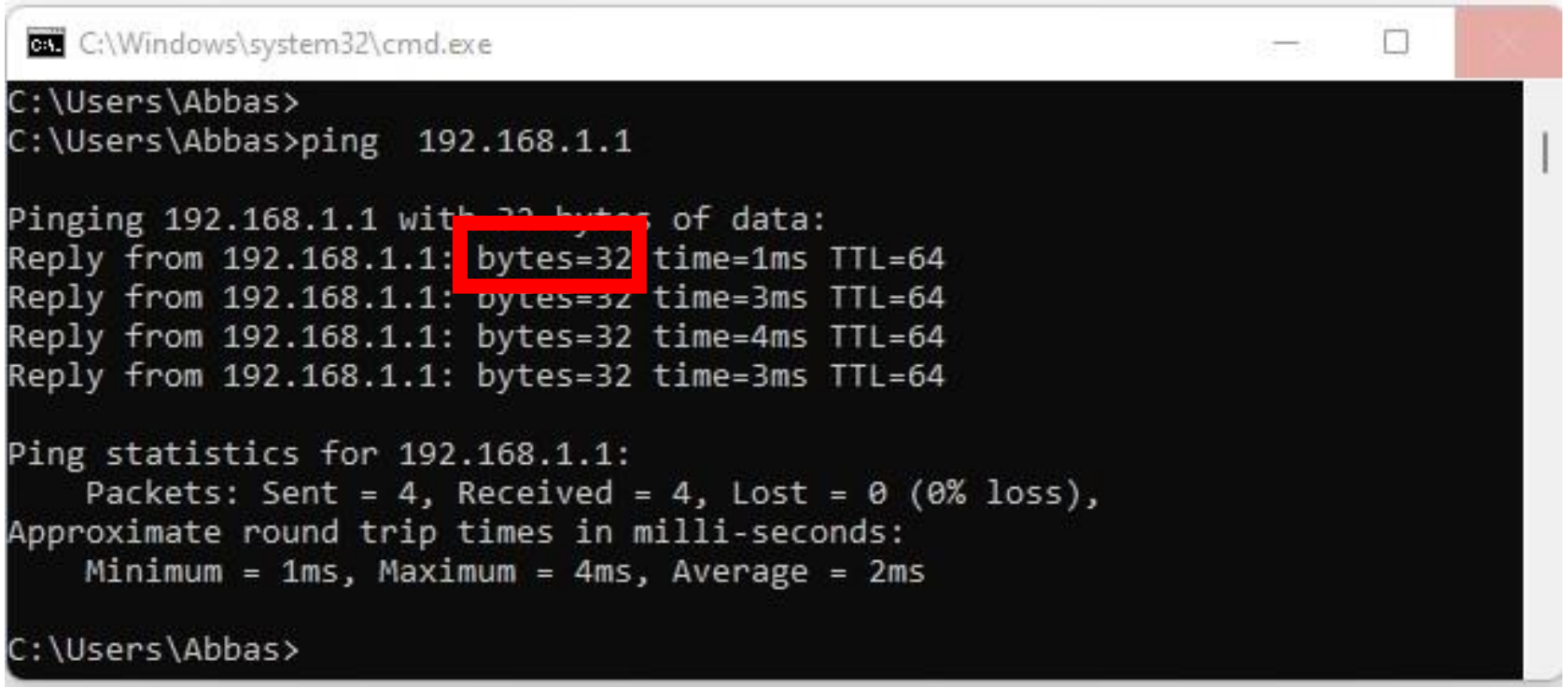
Command-Line



- آدرس مقصد

Command-Line

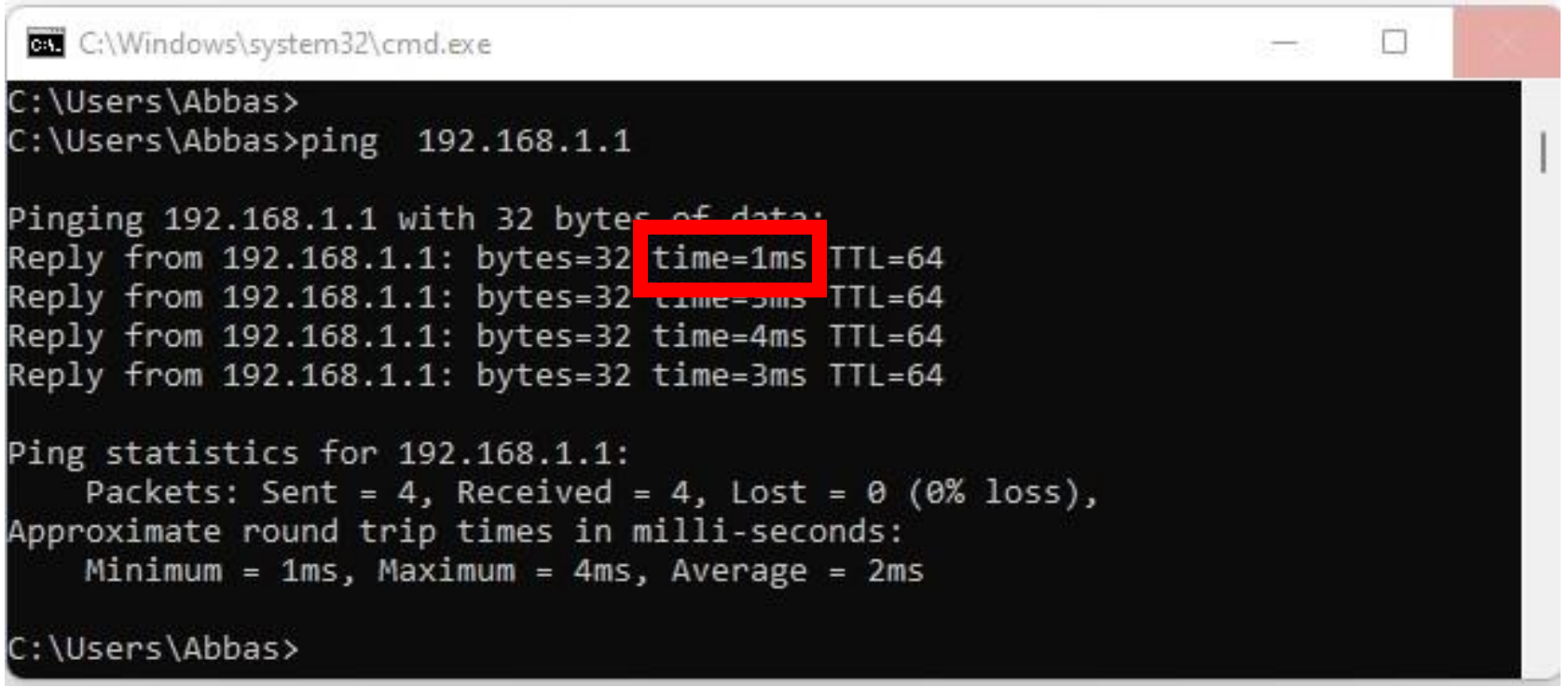
- ping



- حجم پکت

- ping

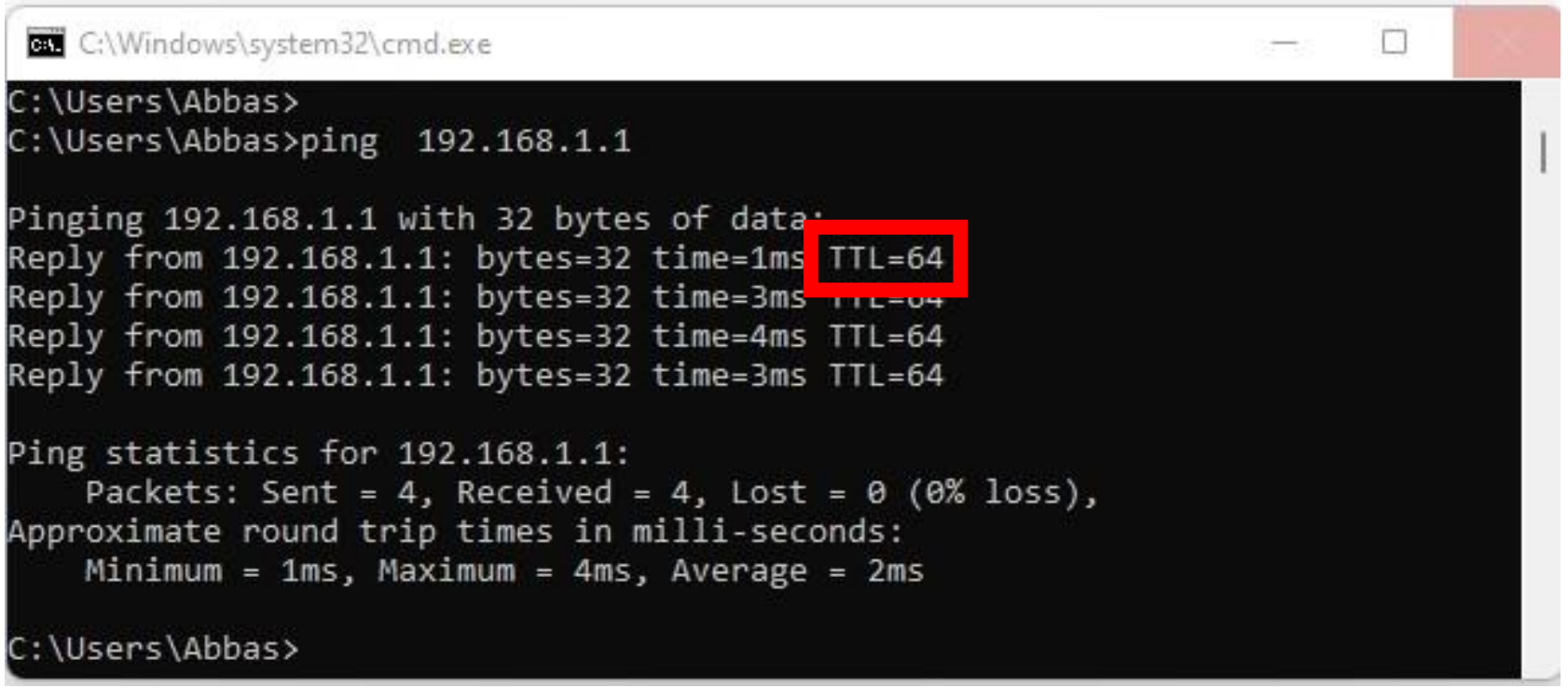
Command-Line



- زمان پاسخ دهی

- ping

Command-Line

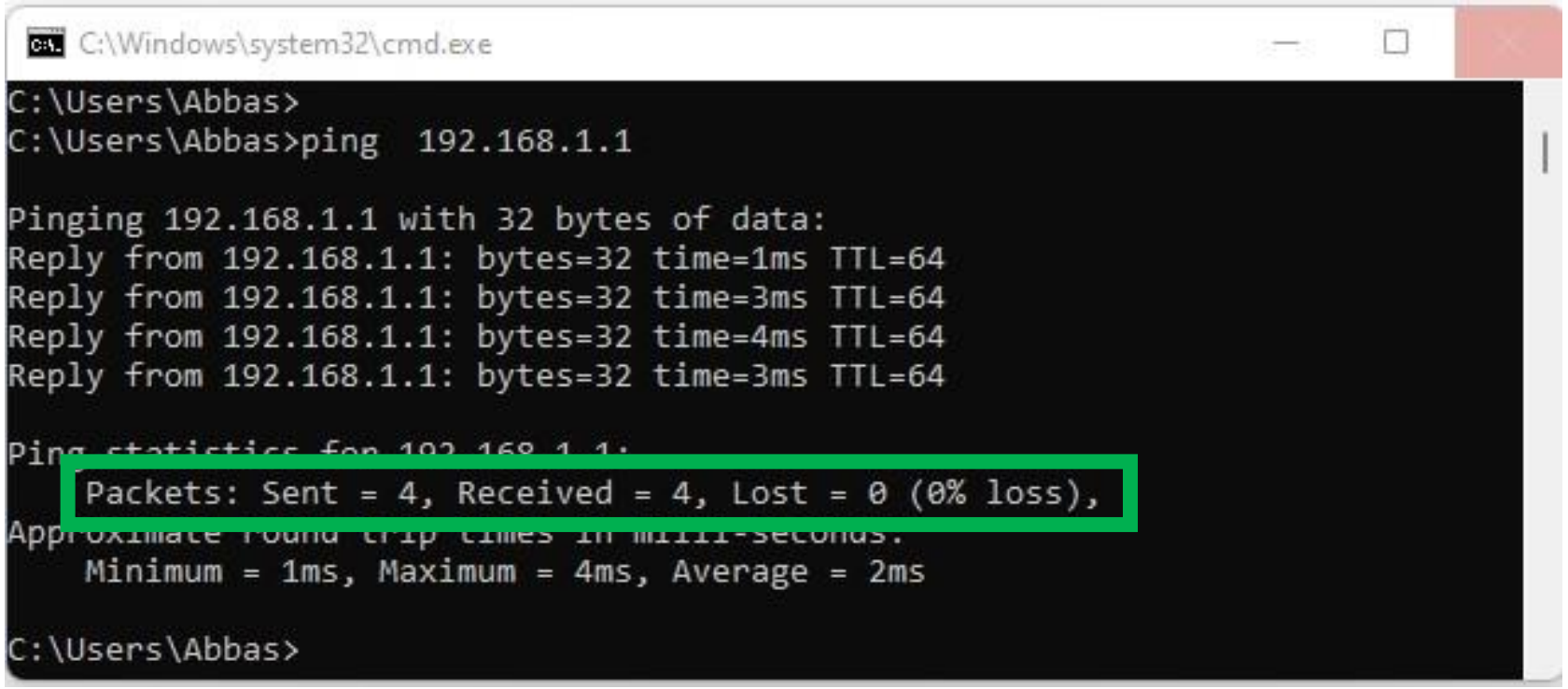


- طول عمر بسته

Time-To-Live ← نمایانگر زمانی است که اگر در طول آن پاسخی دریافت نشود ، بسته دور ریخته خواهد شد

- ping

Command-Line

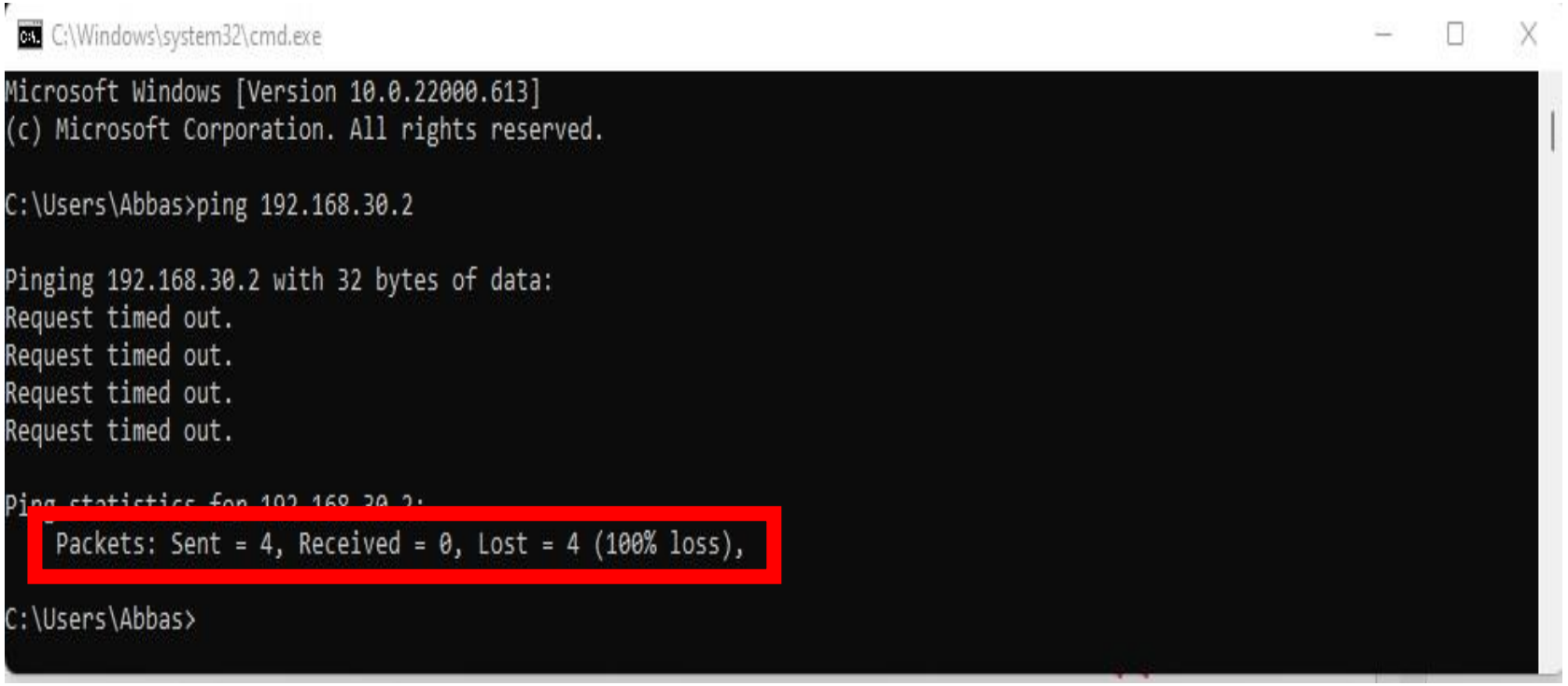


❑ نتیجه

پکت ها به درستی ارسال و دریافت شد و هیچ پکت از دست رفته ای نداریم

- ping

Command-Line -



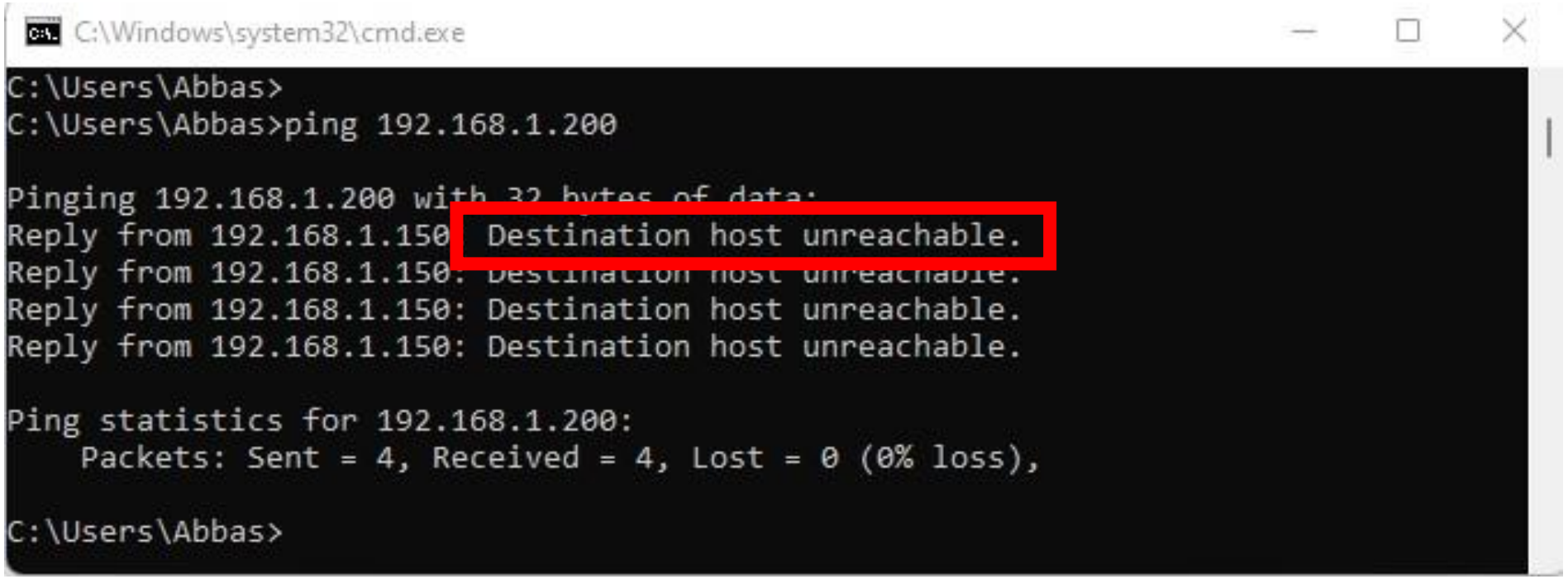
❑ نتیجه

پکت ها ارسال شد اما هیچ پاسخی دریافت نشد و همه پکت از دست رفته است

- ping

Command-Line

-



❑ نتیجه

مقصد مورد نظر در دسترس و یا موجود نیست (امکان دارد سیستم مقصد خاموش باشد)

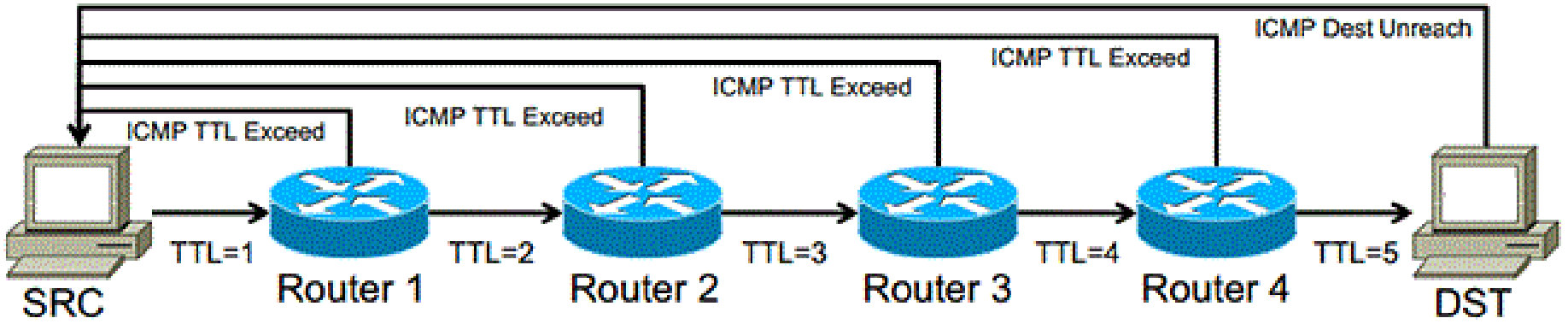
Command-Line

- ✓ جهت مشخص کردن مسیر عبوری بسته

- **tracert** **-d** → فقط نمایش IP ها هنگام بررسی مسیر
  -h count → عبور از تعداد مشخصی روتر
  target-name

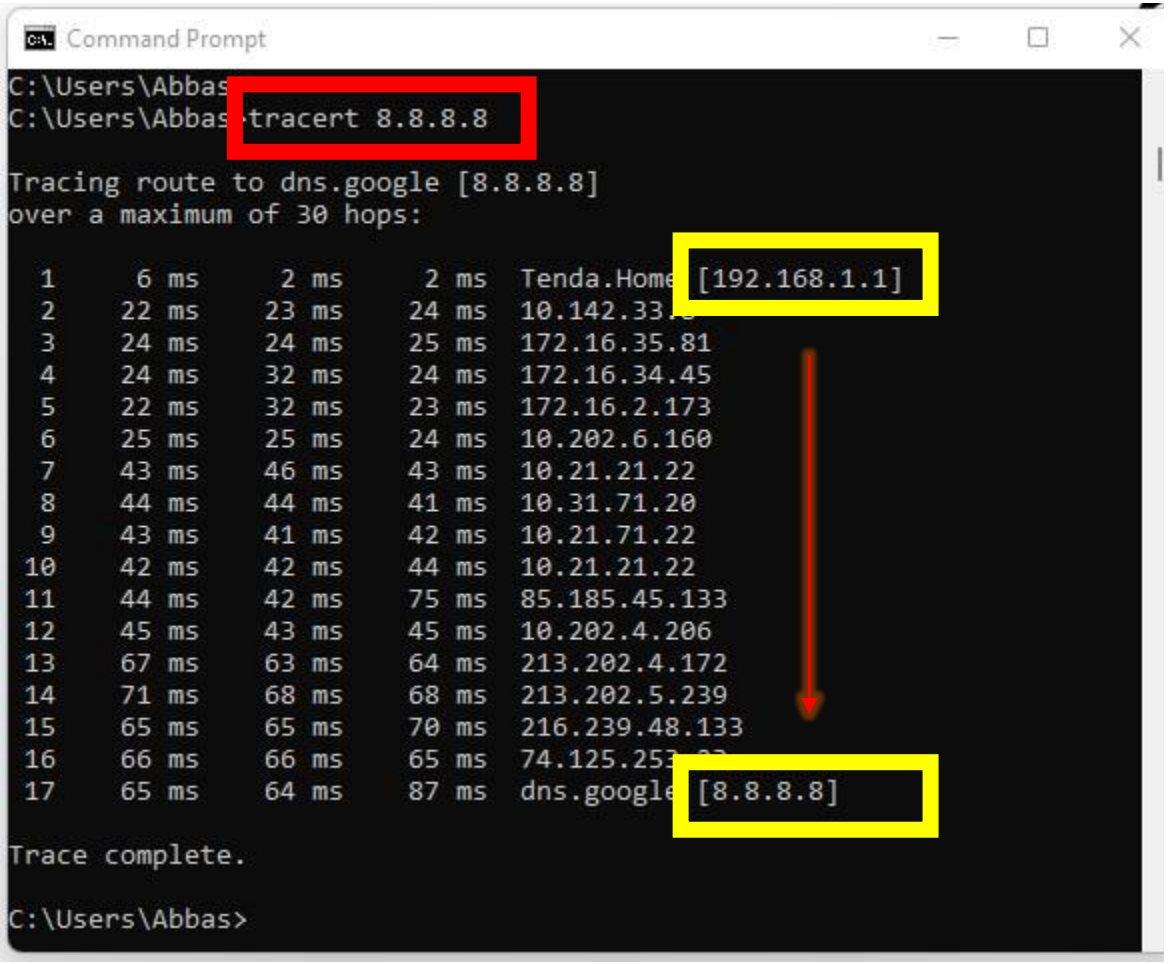
Command-Line

- tracert



Command-Line

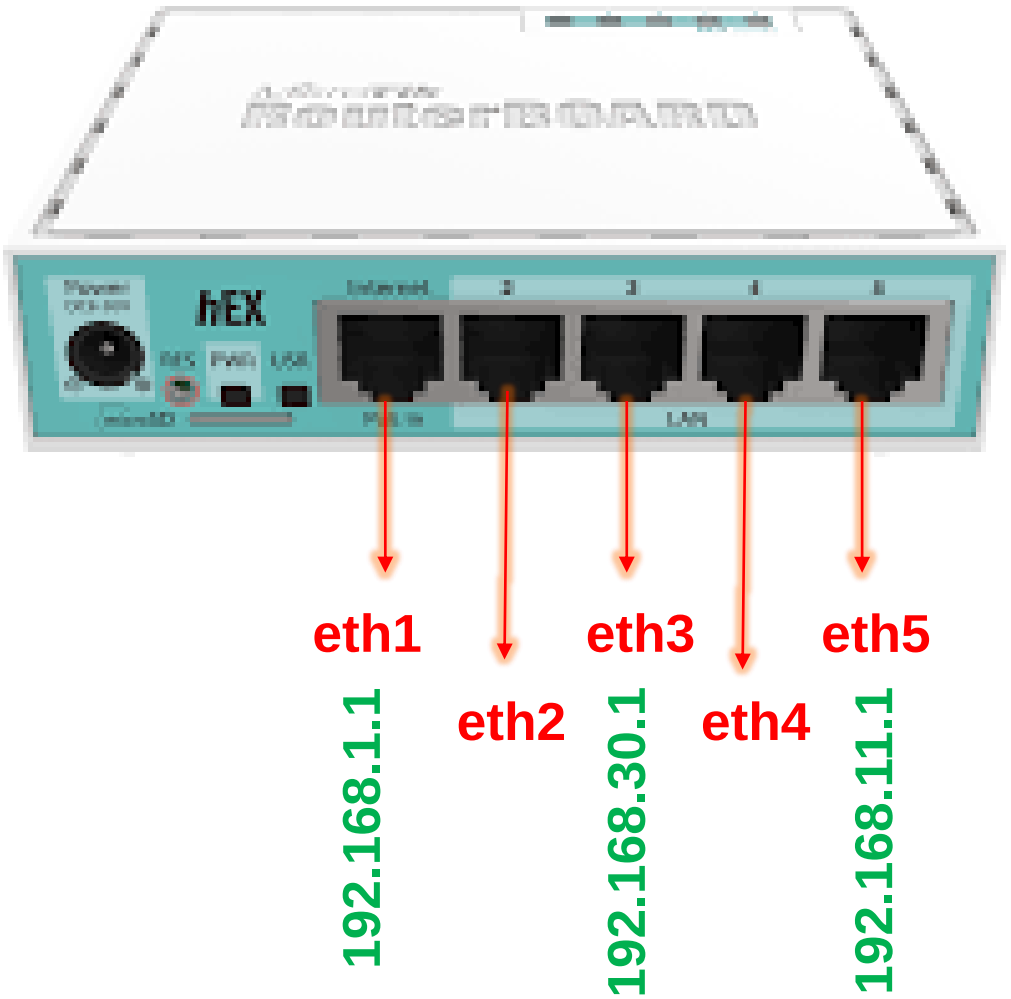
- tracert



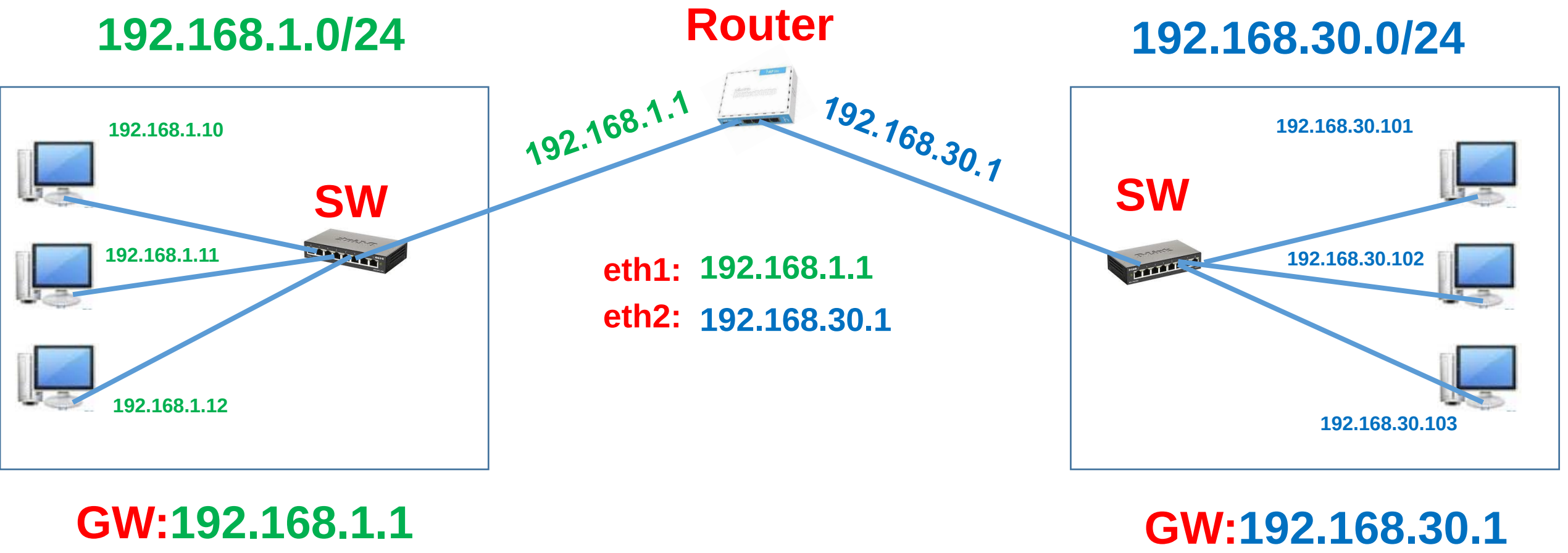
Routing

- ✓ به فرآیند تصمیم‌گیری برای انتخاب مسیر مناسب برای بسته‌های ارسالی گفته می‌شود
- ✓ به تجهیزاتی که عمل روتینگ را انجام میدهند روتر(Router) گویند

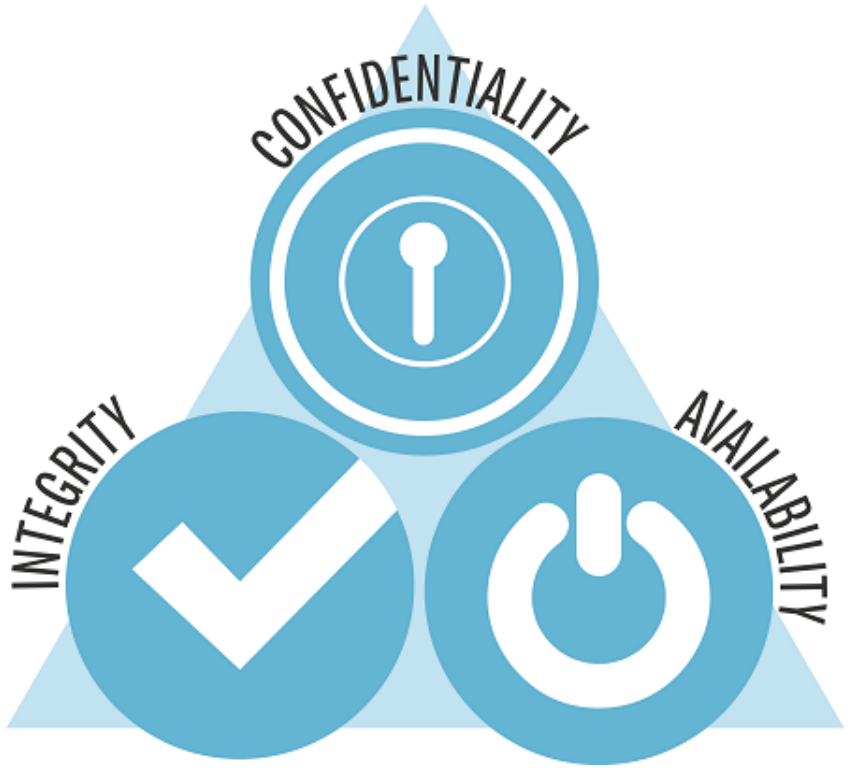
Routing



Routing


192.168.1.0/24
Router
192.168.30.0/24
192.168.1.10
SW
192.168.1.11
192.168.1.12
192.168.1.1
192.168.30.1
eth1: 192.168.1.1
eth2: 192.168.30.1
192.168.30.101
SW
192.168.30.102
192.168.30.103
GW:192.168.1.1
GW:192.168.30.1

Network Security ❑



Network Security ❑

سه هدف اصلی امنیت شبکه

1- Confidentiality → محرمانه بودن

2- Integrity → یکپارچگی

3- Availability → در دسترس بودن

Confidentiality

محرمانه بودن

- **محرمانه بودن داده ها به معنای خصوصی نگه داشتن آنهاست.**

محدود کردن دسترسی به داده ها

- **فیزیکی** ← جداسازی کامل سیستم از شبکه
- **منطقی** ← **VLAN** بندی شبکه و اعمال محدودیت

- **Confidentiality**

محرمانه

- **مکانیزم های محرمانه کردن شبکه:**

✓ استفاده از فایروال ها و لیست های کنترل دسترسی

✓ استفاده از نام کاربری و رمز عبور برای دسترسی به منابع خاص شبکه

✓ رمزگذاری ترافیک جهت عدم دسترسی مهاجم خارج از شبکه

- **Integrity**

یکپارچگی

- **یکپارچگی داده ها تضمین می کند که:**

✓ داده ها در حین انتقال تغییر نکنند

✓ عملیات، کامل و بدون نقص انجام گیرد

پروسه و رهگیری یک خرید اینترنتی

- **Availability**

  در دسترس بودن

- **معیاری برای دسترسی به داده ها در شبکه می باشد**

مثال:

اگر سروری تنها ۵ دقیقه در سال از کار بیفتد، سرور ۹۹.۹۹۹ درصد در دسترس خواهد بود.

- **Availability**

در دسترس بودن

تلاش برای از دسترس خارج کردن سیستم های یک شبکه:

- ✓ ارسال اطلاعات با فرمت نامناسب به یک دستگاه شبکه و ایجاد خطا در آن
- ✓ ارسال سیل عظیم درخواست و ایجاد ترافیک بسیار بالا به یک شبکه

Availability

در دسترس بودن

سیاستهای موجود جهت در دسترس نگه داشتن سرور در شبکه:

- **redundancy (افزونگی)**

Power supply

- **Availability**

در دسترس بودن

سیاستهای موجود جهت در دسترس نگه داشتن سرور در شبکه:

- ❖ **redundancy (افزونگی)**

NIC

- **Availability**

در دسترس بودن

سیاستهای موجود جهت در دسترس نگه داشتن سرور در شبکه:

❖ **redundancy (افزونگی)**

DISK

- **Availability**

در دسترس بودن

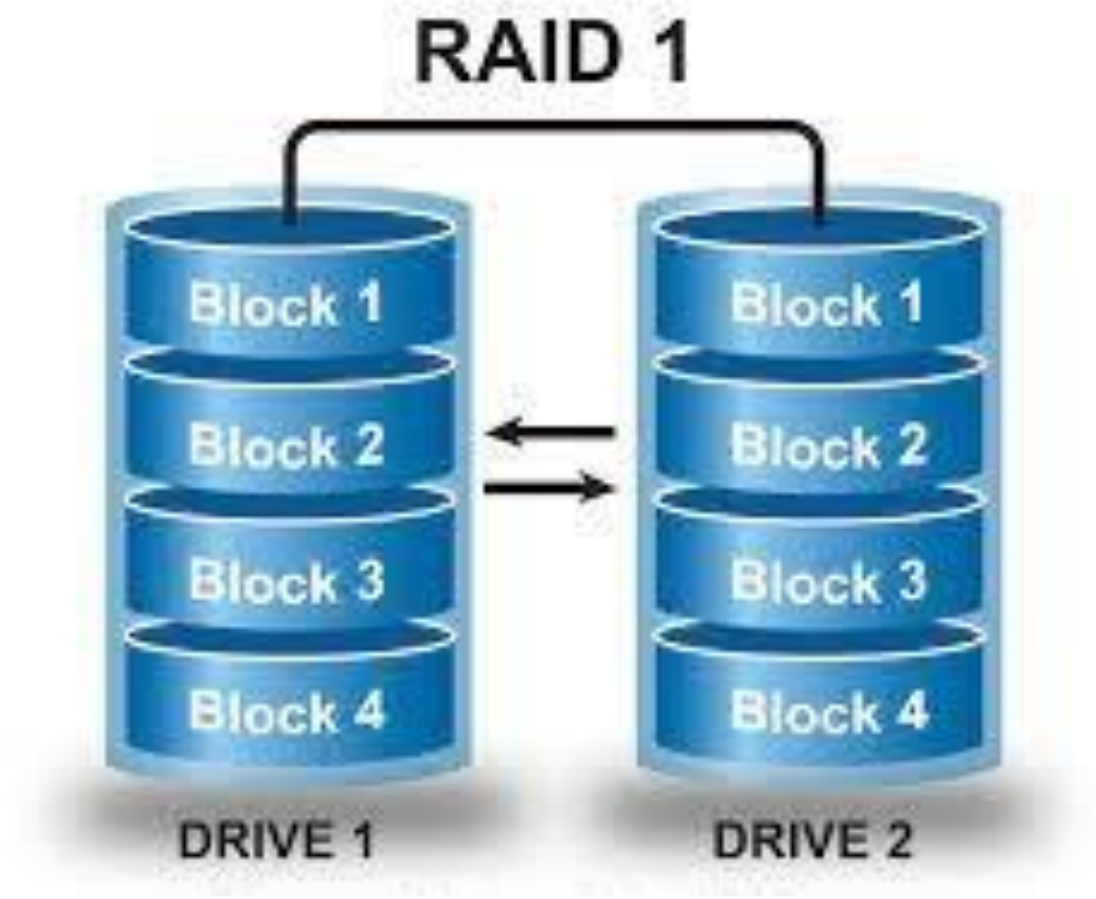
سیاستهای موجود جهت در دسترس نگه داشتن سرور در شبکه:

❖ **redundancy** (افزونگی)

RAID ← **redundant array of independent disks**

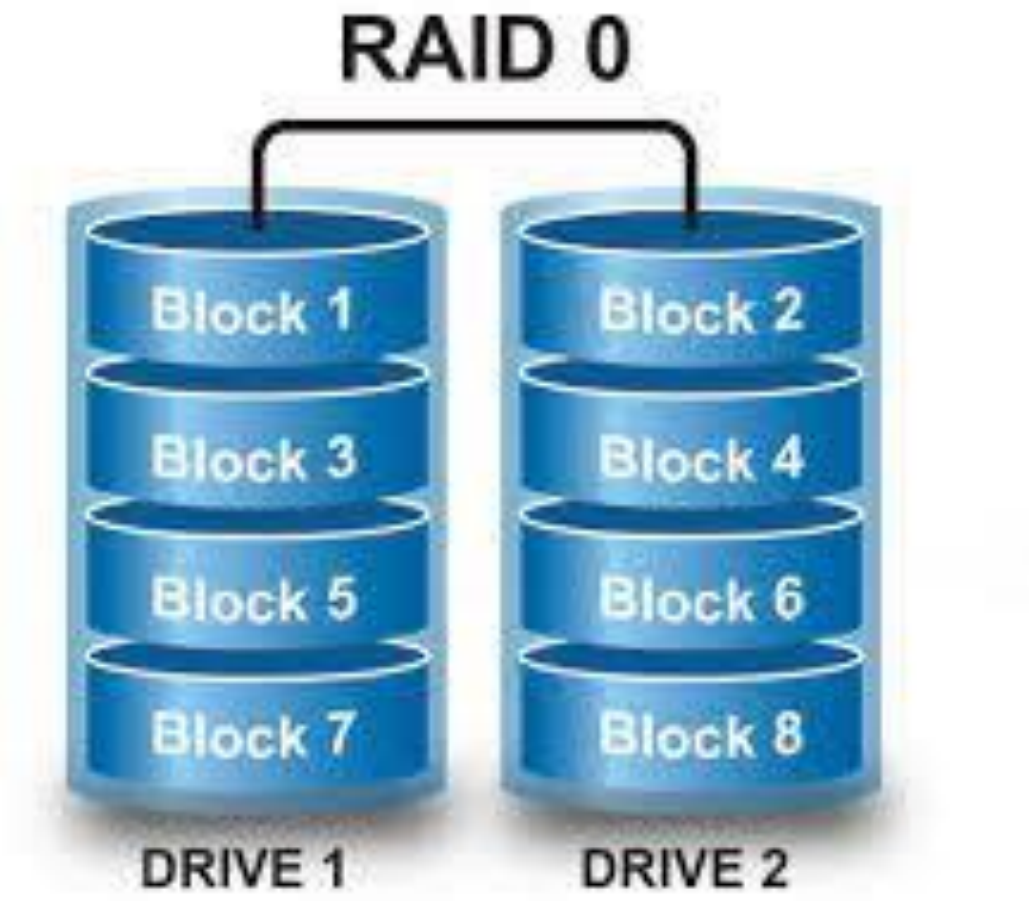
آرایه ای از دیسک های مستقل

RAID ▪



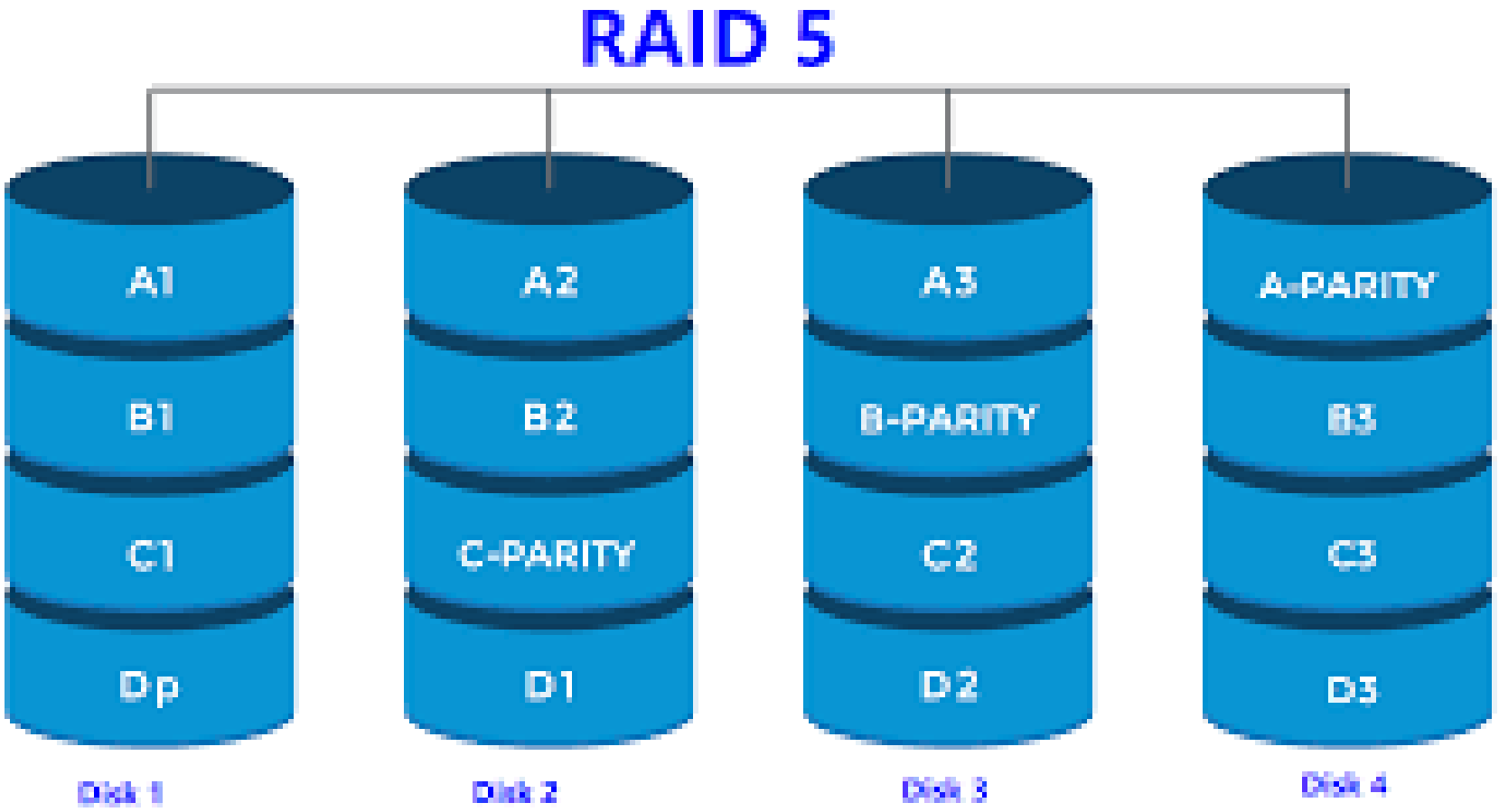
Mirrored Volume

RAID ▪



Striped Volume

RAID ▪


RAID 5
A1
B1
C1
Dp
A2
B2
C-PARITY
D1
A3
B-PARITY
C2
D2
A-PARITY
B3
C3
D3
Disk 1
Disk 2
Disk 3
Disk 4

❑Wireless LANs

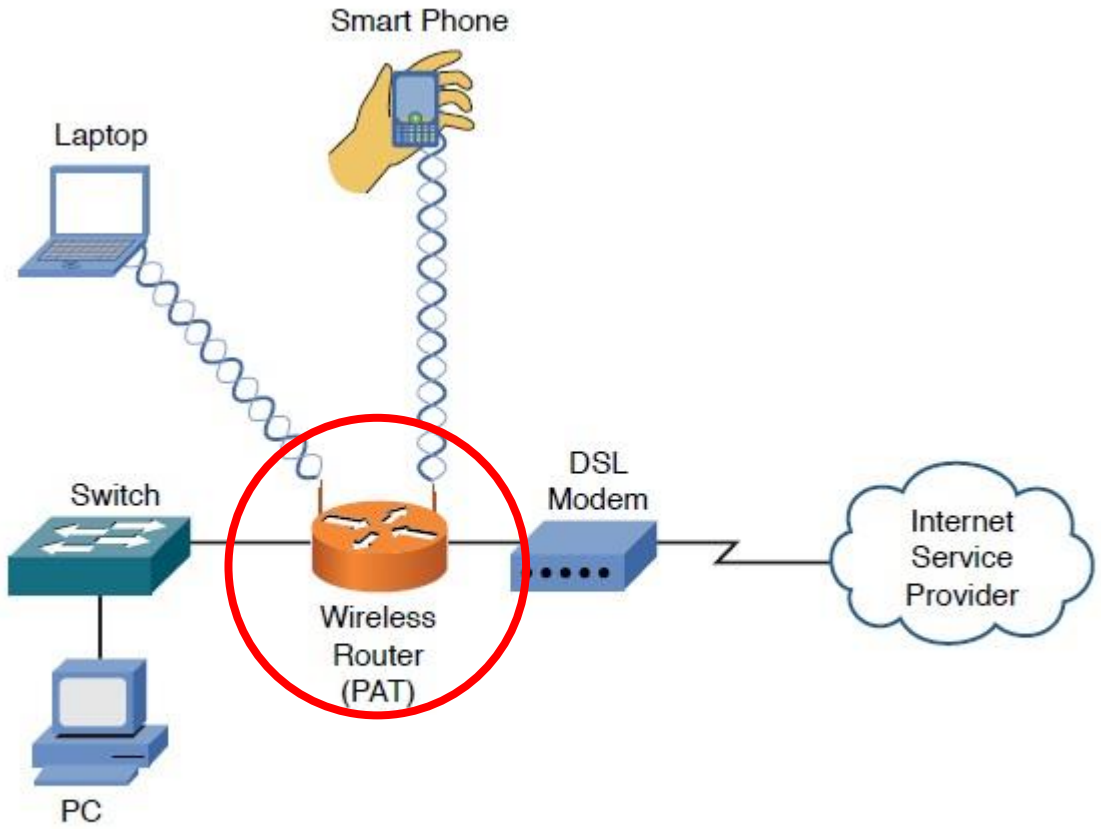
- مفاهیم و اجزای WLAN

یک کلاینت بی سیم به یک ایستگاه پایه بی سیم مانند اکسس پوینت یا یک روتر بی سیم متصل می شود

Wireless LANs❑

- مفاهیم و اجزای WLAN

Wireless Routers

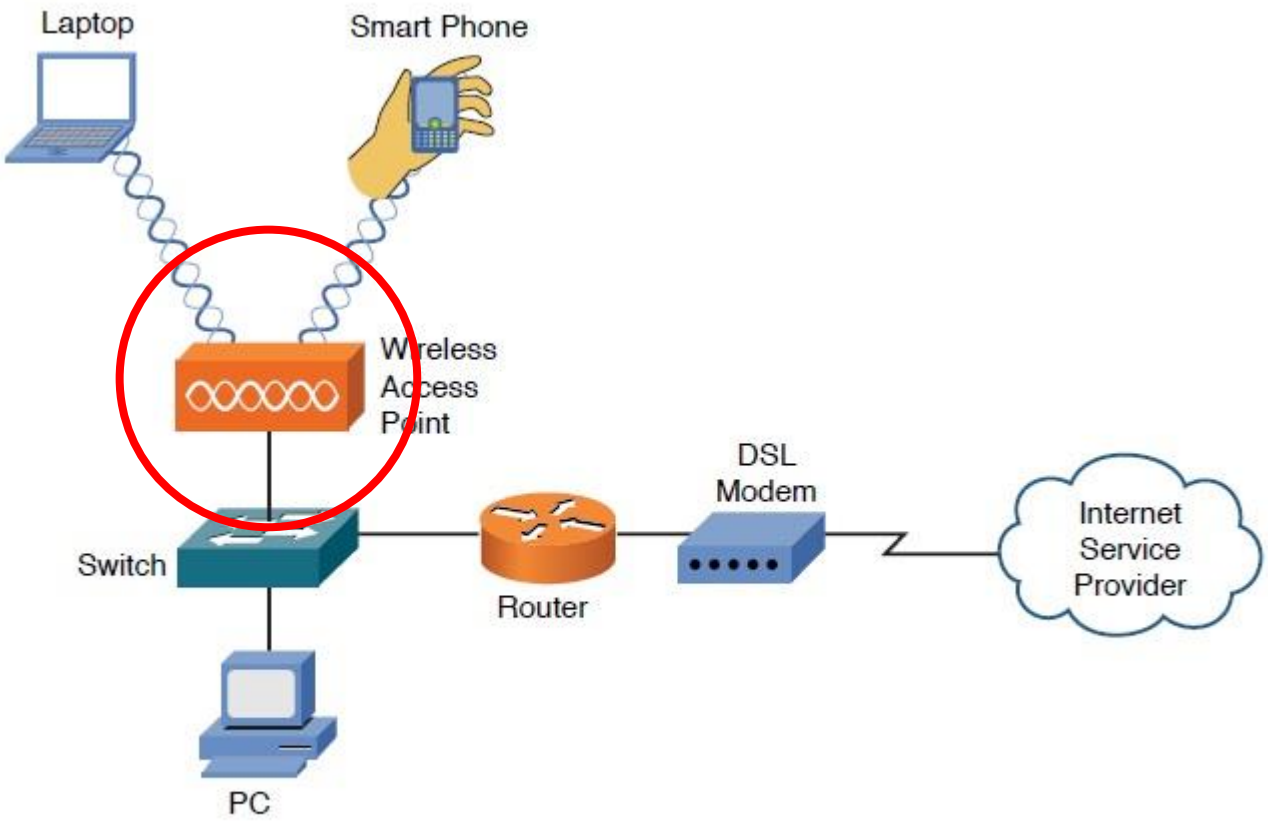


Basic WLAN Topology with a Wireless Router

Wireless LANs❑

- مفاهیم و اجزای WLAN

Wireless Access Point



Basic WLAN Topology with a Wireless AP

❑Wireless LANs

- **Antennas**

اهداف طراحی که هنگام انتخاب آنتن باید در نظر داشت شامل موارد زیر است:

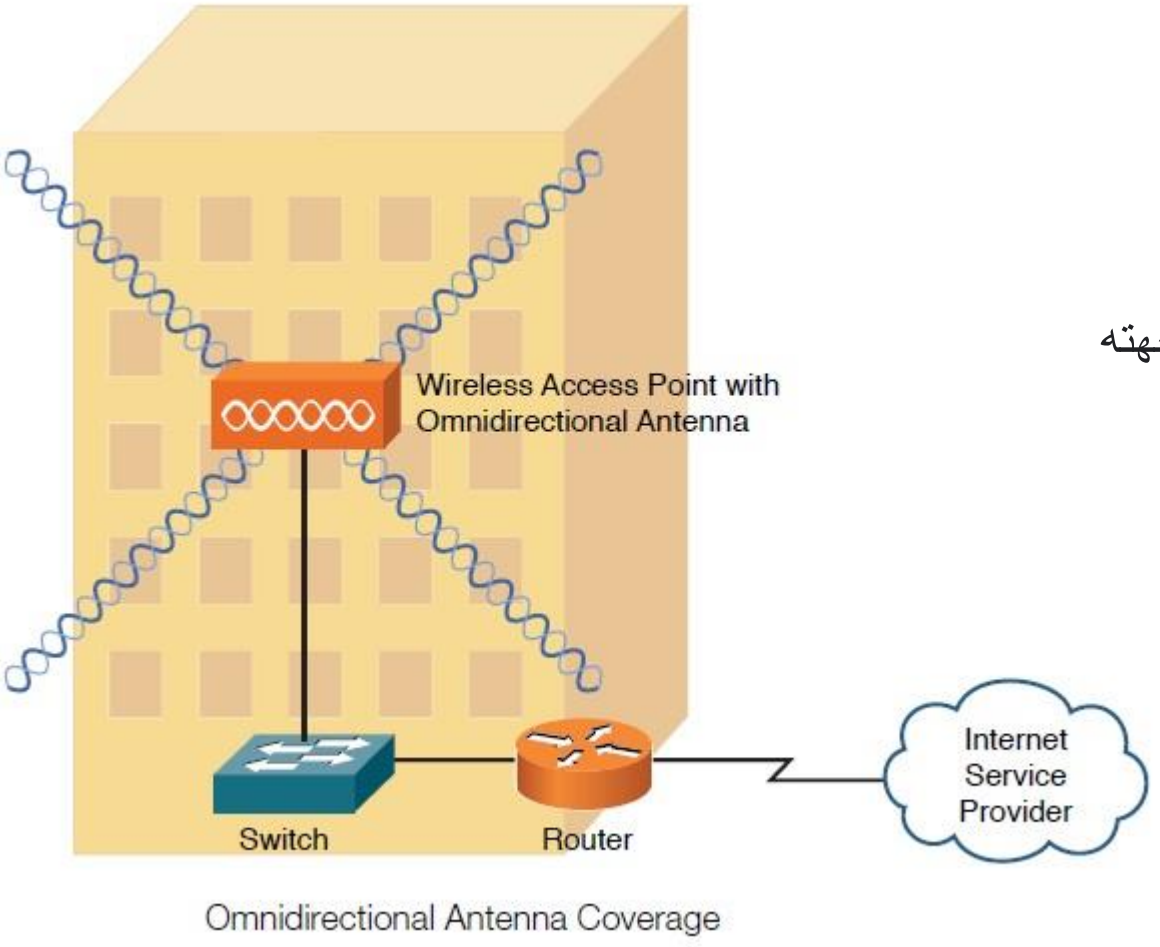
- ✓ فاصله مورد نیاز بین AP و کلاینتها
- ✓ الگوی منطقه تحت پوشش
- ✓ محیط داخلی یا خارجی
- ✓ اجتناب از تداخل با سایر AP ها.

Wireless LANs❑

- **Antennas**

دو دسته گسترده از آنتن ها:

✓ Omnidirectional ← همه جهته

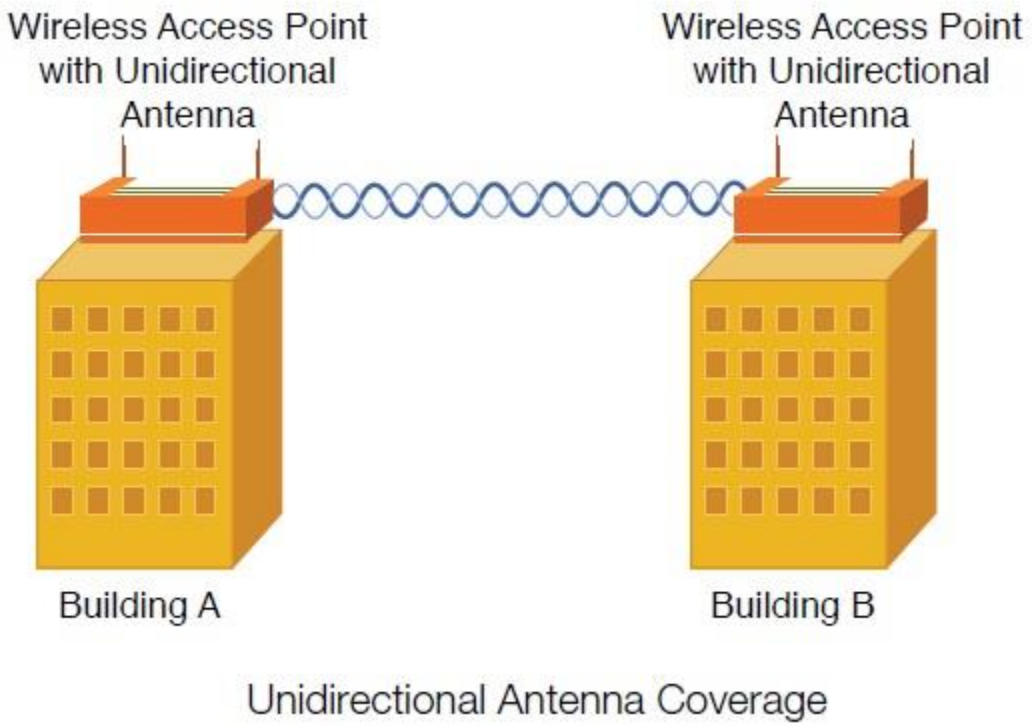


Omnidirectional Antenna Coverage

Unifi

Wireless LANs❑

Antennas ▪



Unidirectional Antenna Coverage

دو دسته گسترده از آنتن ها:

✓ Unidirectional ← یک طرفه

SXT

❑Wireless LANs

▪ Frequencies and Channels

باندهای فرکانسی

✓ گستره‌ای از امواج رادیویی هستند که از آنها برای انتقال داده ها در بسامد ارتباط بی سیم استفاده میشود.

➢ هرچقدر فرکانس بالاتر باشد، سرعت انتقال هم بالاتر میرود

➢ هرچقدر گستره‌ی امواج کوتاه‌تر میشه و پوشش کاهش پیدا می‌کنه

Wireless LANs❑

Frequencies and Channels ▪

Industrial **Scientific** **Medical** ← **ISM bands** ✓

محدوده باندهای فرکانسی خاصی که در سطح بین المللی برای اهداف صنعتی، علمی و پزشکی رزرو شده است

Wireless LANs❑

▪ Frequencies and Channels

باندهای مخصوص شبکه های WLAN:

2.4-GHz to 2.5-GHz ← **2.4-GHz band** ✓

5.725-GHz to 5.875-GHz ← **5-GHz band** ✓

❑Wireless LANs

▪ Frequencies and Channels

✓ 2.4-GHz band

- ➢ منطقه‌ی وسیعی را پوشش میدهد
- ➢ نرخ تبادل اطلاعات نسبتا پایینی دارد
- ➢ این باند بسته به نوع دستگاه، سرعت ۴۵۰ تا ۶۰۰ مگابیت بر ثانیه را ساپورت می‌کند
- ➢ راحت از دیوار و اجسام سخت عبور می‌کند و محدوده‌ی بزرگ‌تری را پوشش میدهد

نکته منفی این باند فرکانسی ← تراکم چشمگیراین فرکانس به دلیل استفاده‌ی زیاد است

علاوه بر wifi، در عملکرد مایکروویو، درب اتوماتیک، تلفن بی‌سیم و دستگاه‌های بلوتوثی هم مشکل ایجاد می‌کند

Wireless LANs❑

▪ Frequencies and Channels

5-GHz band ✓

- ➢ این باند پرسرعت برای پوشش محدوده‌های کوچک طراحی شده است
- ➢ نرخ تبادل اطلاعات نسبتا بالایی دارد
- ➢ سرعت انتقال دیتا به ۱۳۰۰ مگابیت بر ثانیه میرسد
- ➢ قدرت نفوذ این فرکانس در اجسام سختی مثل دیوار، نسبتا پایین است

نکته مثبت این باند فرکانسی ← اختلال کم در شبکه به دلیل استفاده‌ی کمتر از این باند است

Wireless LANs❑

▪ WLAN Standards

استاندارد ۸۰۲.۱۱ ← عموما آن را به عنوان Wi-Fi میشناسند

- ✓ اولین بار در سال ۱۹۹۷ توسط انجمن مهندسان برق و الکترونیک (IEEE) بعنوان اولین استاندارد بین المللی شبکه های محلی بیسیم (WLAN) ارائه شد.

Wireless LANs❑

WLAN Standards ▪

Standard	Band	Max. Bandwidth
802.11	2.4 GHz	1 Mbps or 2 Mbps
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz or 5 GHz (or both)	> 300 Mbps (with channel bonding)
802.11ac	5 GHz	> 3 Gbps (with MU-MIMO and several antennas)

۸۰۲.۱۱ a
۸۰۲.۱۱ g
۸۰۲.۱۱ b
۸۰۲.۱۱ n
۸۰۲.۱۱ ac

محبوب ترین انواع
استاندارد ۸۰۲.۱۱

Wireless LANs❑

Types of WLANs ▪

- Independent Basic Service Set (IBSS) → مجموعه خدمات پایه مستقل
- Basic Service Set (BSS) → مجموعه خدمات پایه
- Extended Service Set (ESS) → مجموعه خدمات گسترده

Wireless LANs❑

Types of WLANs ▪

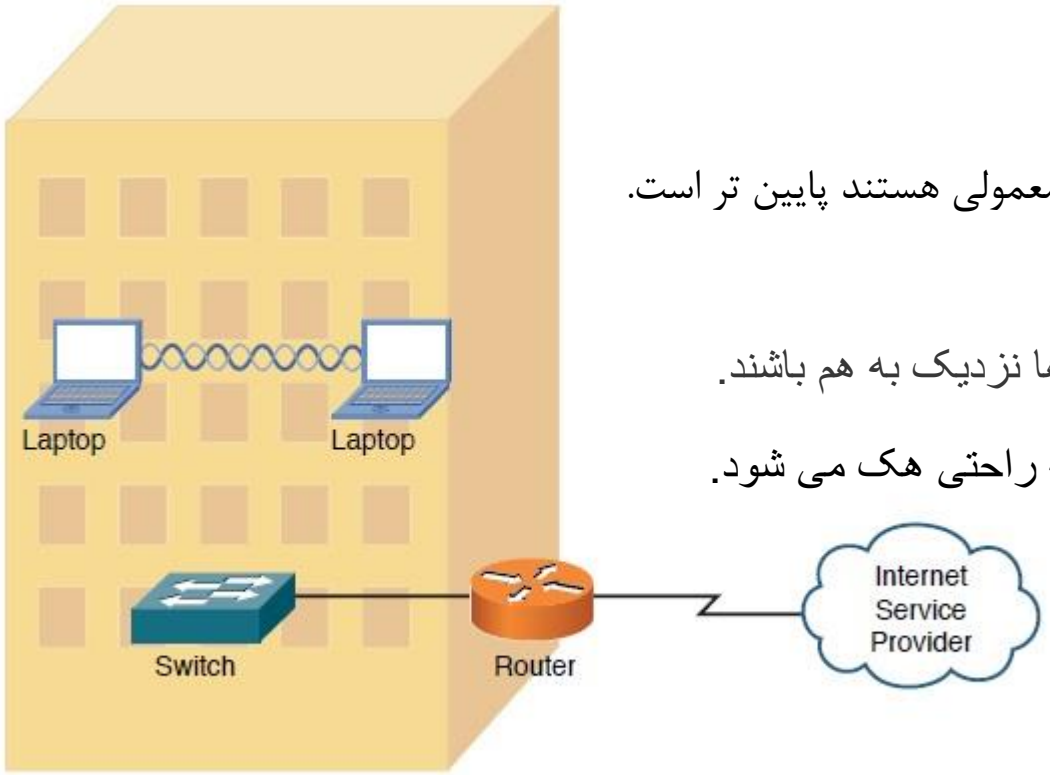
IBSS ➢

۱- سرعت یک شبکه ی Ad-hoc معمولا از شبکه هایی که دارای یک زیرساخت معمولی هستند پایین تر است.

۲- سرعت این شبکه ها حداکثر به 11 Mbps می رسد.

۳- قدرت سیگنال در شبکه های ad-hoc زیاد نیست ، بنابراین باید لپ تاپ ها نزدیک به هم باشند.

۴- به علت اینکه از زیرساخت های معمولی امنیتی نیز پشتیبانی نمی کند ، به راحتی هک می شود.



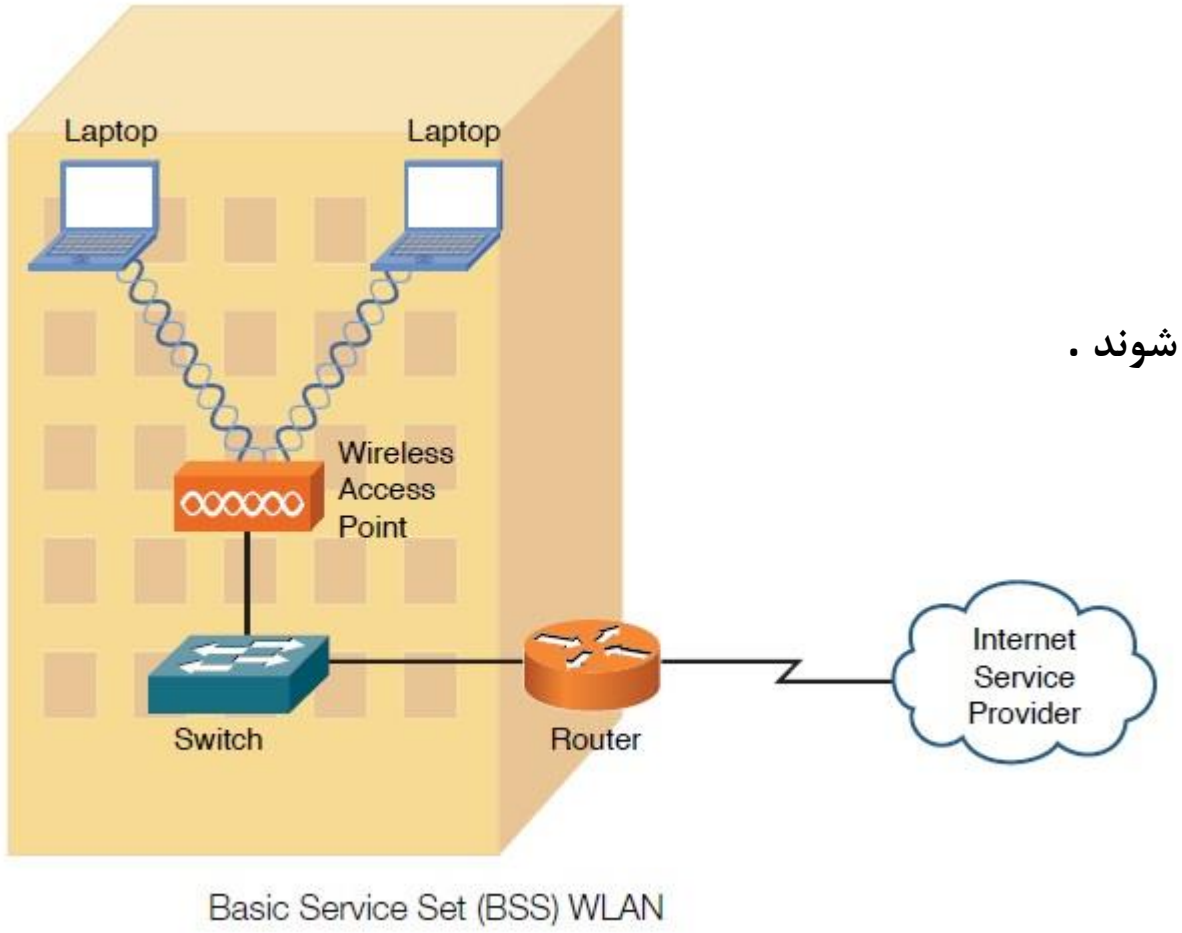
Independent Basic Service Set (IBSS) WLAN

Wireless LANs❑

Types of WLANs ▪

BSS ➢

✓ WLAN هایی که فقط یک AP دارند، BSS WLAN نامیده می شوند .



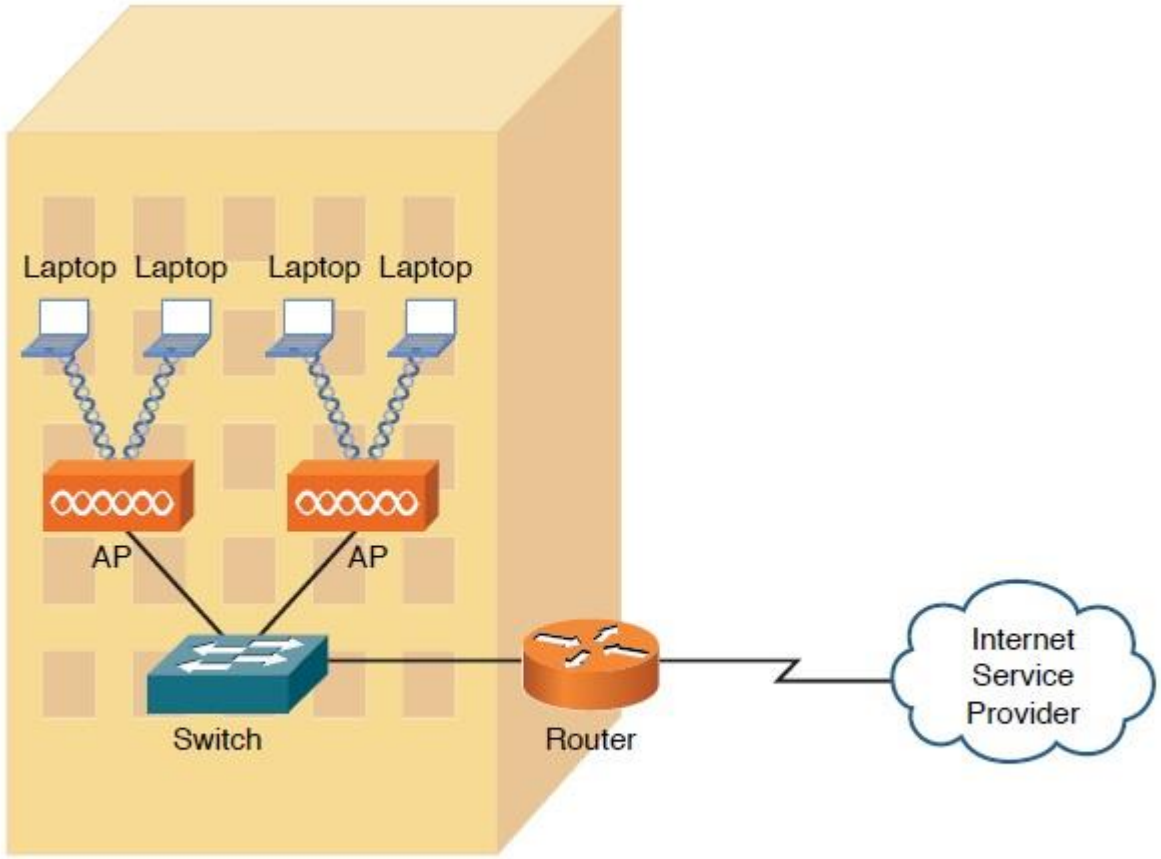
Basic Service Set (BSS) WLAN

Wireless LANs❑

Types of WLANs ▪

ESS ➢

✓ **WLAN** های حاوی بیش از یک **AP** را **ESS WLAN** می نامند.



Extended Service Set (ESS) WLAN

❑Wireless LANs

▪ Types of WLANs

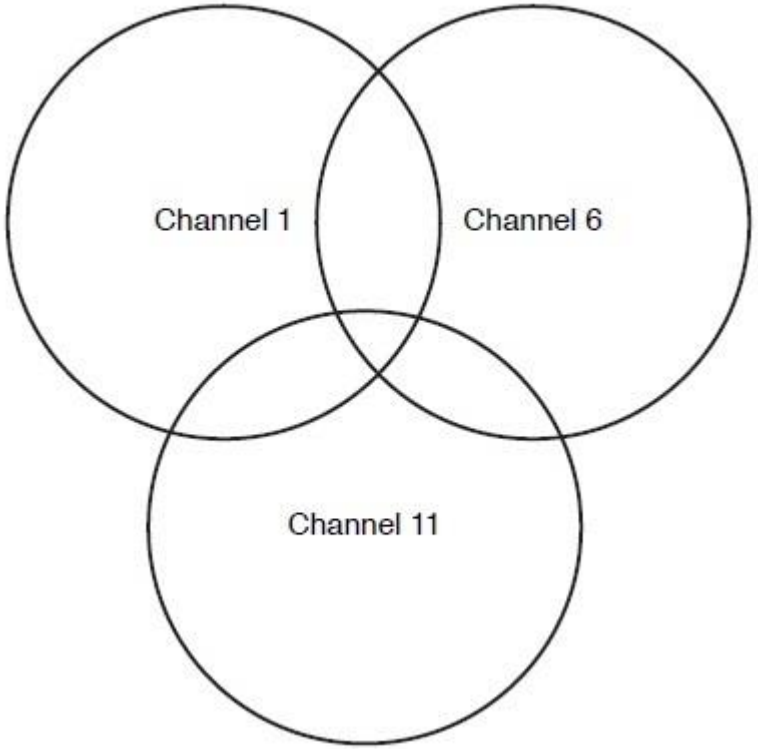
❖ قرار دادن چندین AP

- ✓ یک پوشش همپوشانی بین AP ها باید وجود داشته باشد تا امکان رومینگ بدون وقفه از یک سلول که منطقه پوشش ارائه شده توسط یک AP است به سلول دیگر وجود داشته باشد .
- ✓ مناطق تحت پوشش نباید از فرکانس های همپوشانی استفاده کنند

Wireless LANs❑

Types of WLANs ▪

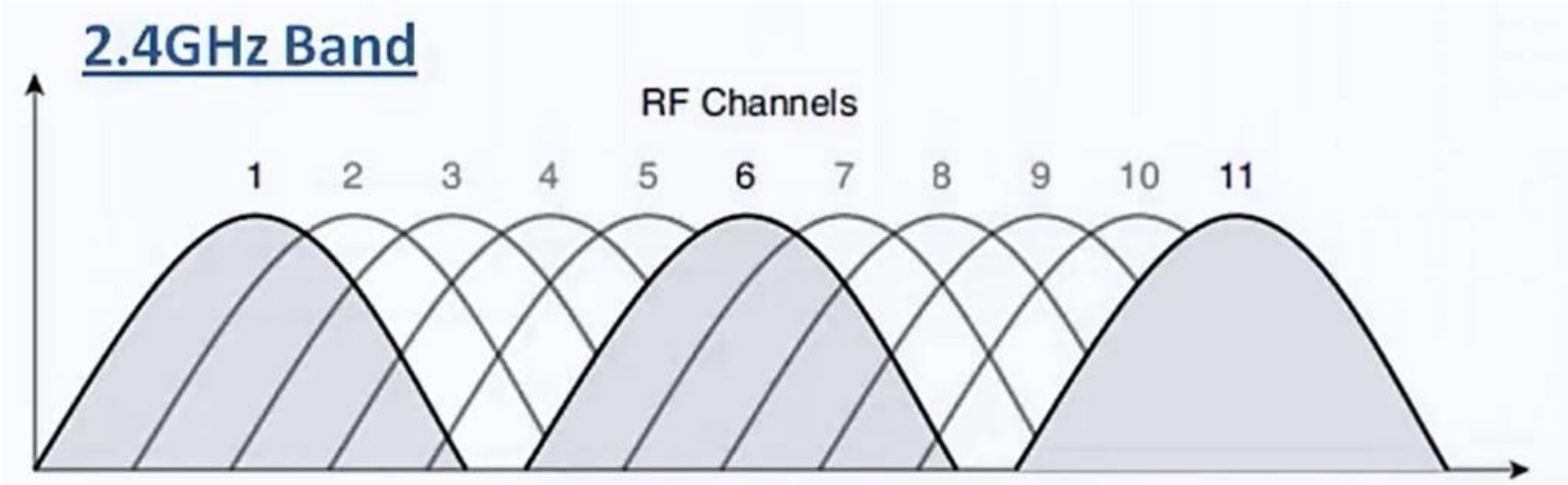
❖ قرار دادن چندین AP



شکل روبرو نشان می دهد که چگونه کانال های غیرهمپوشانی در باند 2.4 گیگاهرتز می توانند مناطق تحت پوشش خود را برای ارائه رومینگ یکپارچه بین مناطق تحت پوشش AP همپوشانی کنند .

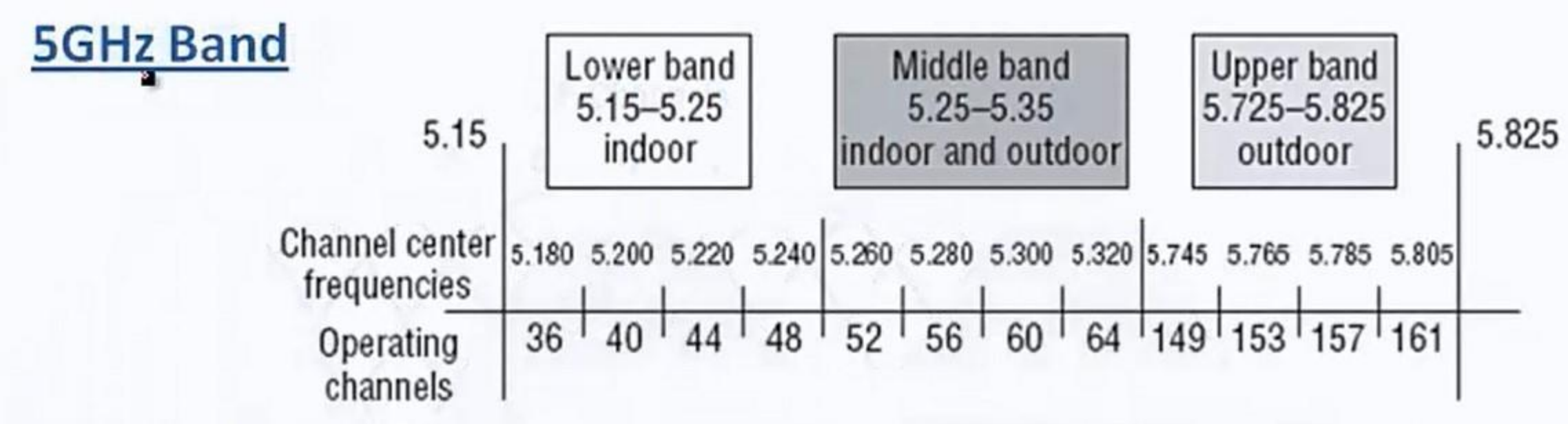
Wireless LANs❑

- **Types of WLANs**
  - ❖ **قرار دادن چندین**AP



Wireless LANs❑

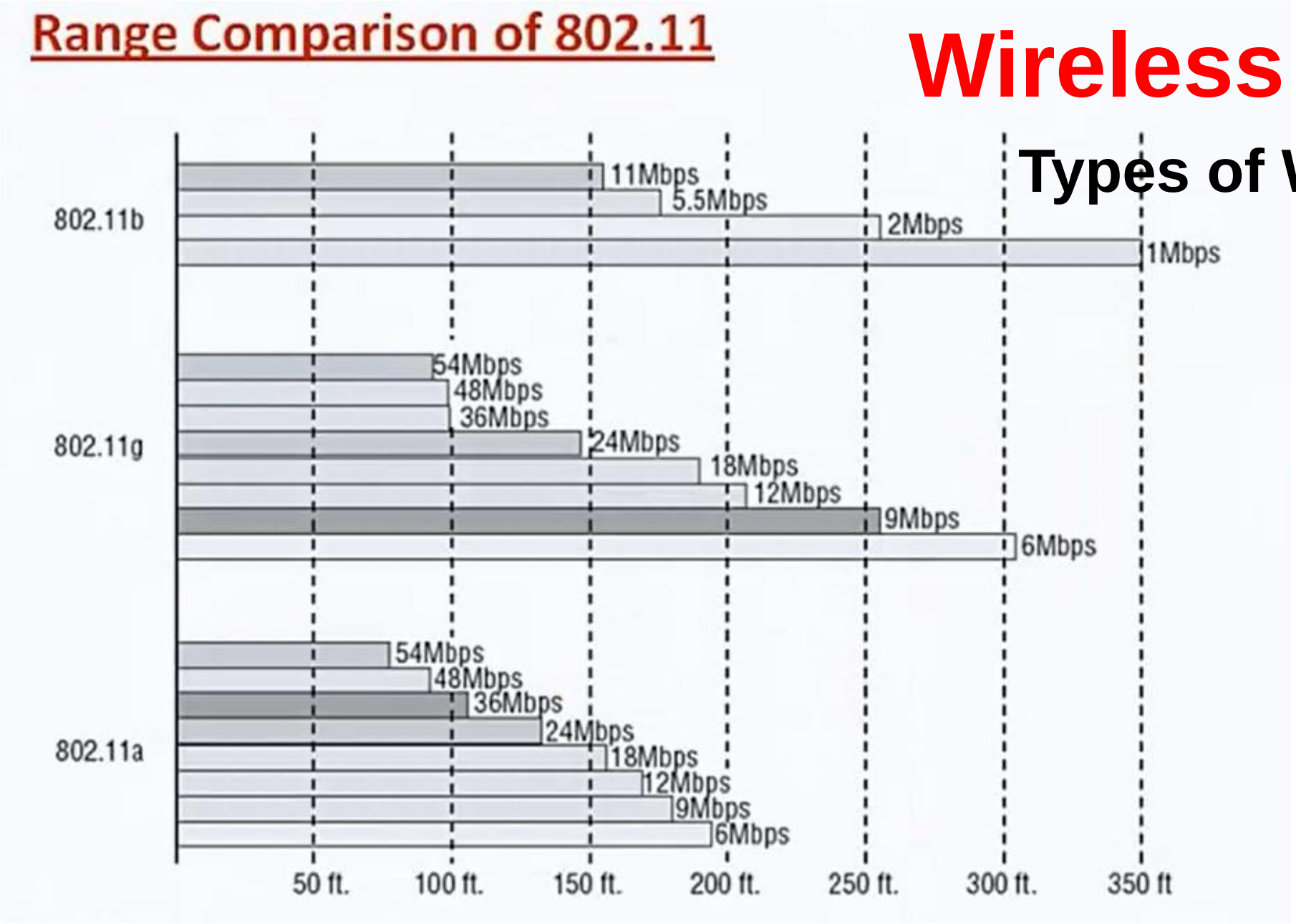
- **Types of WLANs**
  - ❖ **قرار دادن چندین**AP



Wireless LANs❑

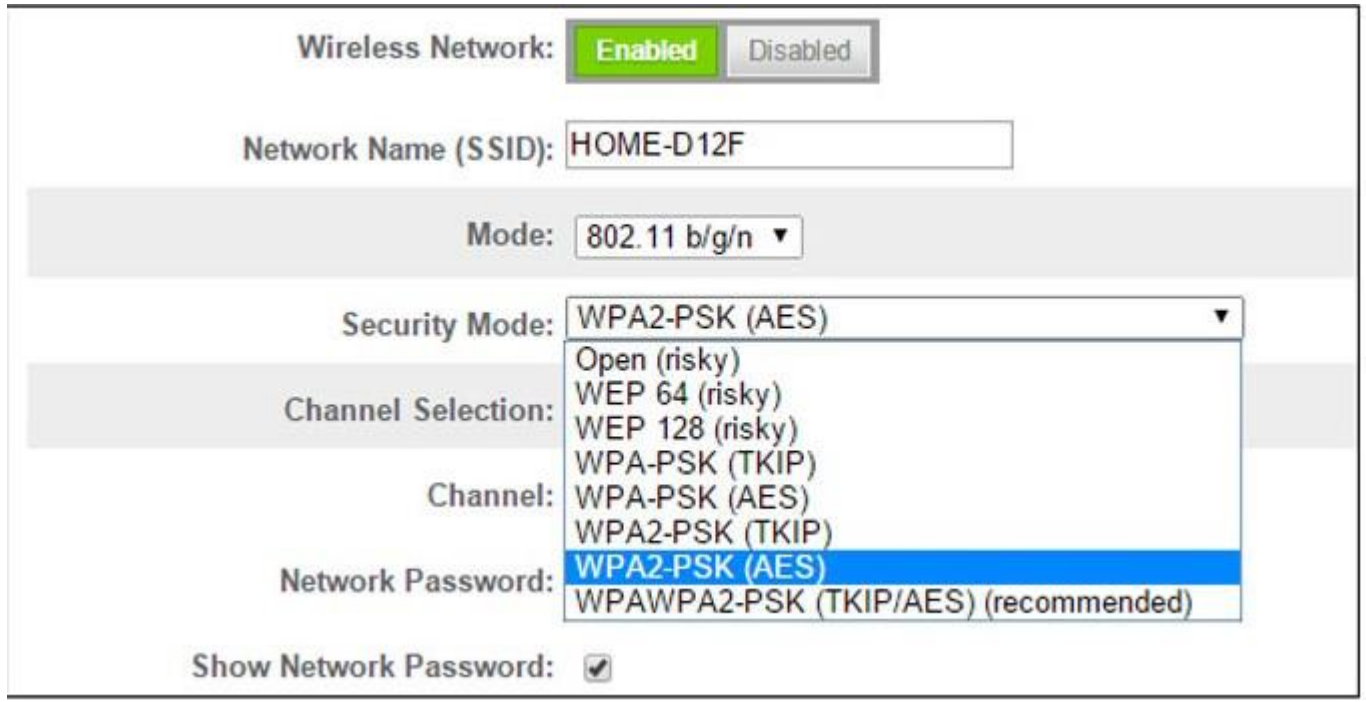
Types of WLANs ▪

✓ هر فوت حدود 30CM



Wireless LANs❑

Security Mode ▪



- **Open**
- **WEP** — Wired Equivalent Privacy
- **WPA** — Wi-Fi protected access
- **WPA2** — Wi-Fi Protected Access 2

Wireless LANs❑

▪ Security Mode

روش های رمز نگاری:

Encryption

مهمترین فاکتور برقراری امنیت در ارتباطات وایرلس رمزنگاری است

- **TKIP**

  Temporal Key Integrity Protocol

  این پروتکل برای جایگزین شدن به جای پروتکل WEP طراحی و پیاده سازی شد

- **AES**

  Advanced Encryption Standard

  استفاده از AES به عنوان یک پروتکل رمزنگاری استاندارد بسیار امن امروزه تایید شده است