NETWORK +

مقدمه :

برای اینکه فرد بهتر بتواند مباحث شبکه را درک کند شرکت COMPTIA با سر فصل NETWORK+ اساس وپایه شبکه را به فرد یاد میدهد.

شبکه : اتصال دو یا بیش از دو کامپیوتر برای اشتراک گذاری منابع

LAN= local area network

WAN=wide area network

InterNetwork = LAN+WAN

Subscriber= مشترکی از یک service provider

Network media

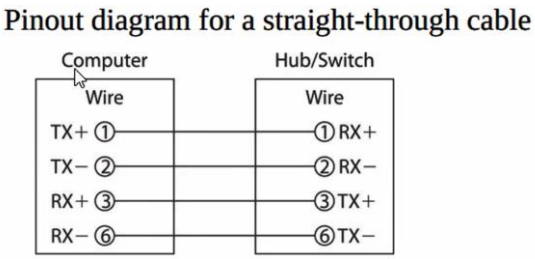
تکنولوژی که به وسیله ی آن host ها را باهم متصل میکند

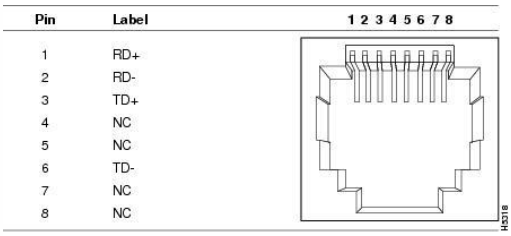
کابلی (copperbase) { coaxial , twisted piar } ، فیبرنوری(fiberoptic) ، بی سیم(wireless)

UTP Categories - Copper Cable

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Firewall.cx





Pin	Label
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC

1 2 3 4 5 6 7 8

CRC Error and input Error how can fix these= **CRC**

چک کردن سیگنال برای خطا یابی و جلوگیری از ایجاد خطا

Power over Ethernet =**POE**

انتقال برق بر روی کابل شبکه

Protocols

قوانینی که host ها با هم به وسیله آن ارتباط برقرار میکنند

- Packet Acknowledgment
- Segmentation
- Flow Control
- Error Detection
- Error Correction
- Data Compression
- Data Encryption

Segmentation = قطعه قطعه کردن داده برای ارسال و دریافت

از کجا آمده ام ، به کجا میروم ، آمدنم بهر چیست ؟

Packet acknowledgement = header اضافه شده که به وسیله آن مبدا و مقصد و شماره بسته مشخص میشود

Flow control = کنترل جریان ، اگر نباشد هاست های یک مجموعه نمیتوانند در آن ارتباط براقرار کنند و فقط کسانی ارتباط خواهند داشت که سرعت آن یکسان خواهد بود

قابلیت اتصال یک host به یک device از طریق قانون flow control

Error detection = تشخیص خطا ، خطای به وجود آمده در شبکه را می یابد

Error correction = تصحیح کردن خطای به وجود آمده

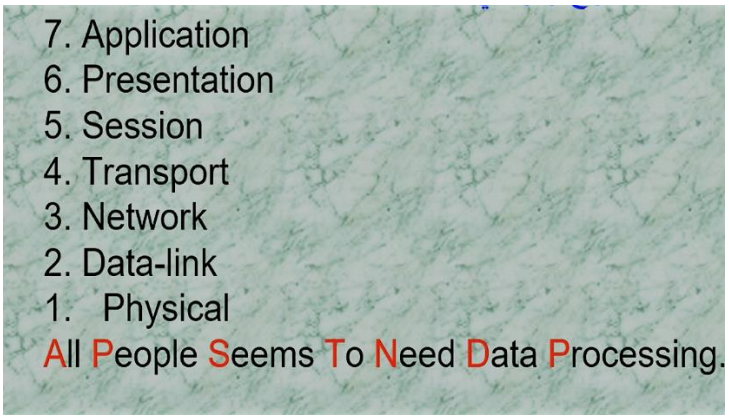
Data compression = فشرده سازی داده ها ، به این علت که در محدوده ارسال ، باید فایل را فشرده سازی کنیم و سپس ارسال کنیم

Data encryption = رمز نگاری ، برای امن کردن اطلاعات استفاده میشود که برای ارسال میشود واز دسترسی افراد غیر مجاز(unauthorized) جلوگیری میکند

برای این که داده امن باشد در ساده ترین حالت کد کردن است تا دیگر افراد نتوانند DATA را بخوانند

مدل OSI

برای شناخت و بهتر دیدن شبکه از مرج مدل OSI استفاده میکنیم که در هفت لایه منطقی logical نحوه کارکرد شبکه را به ما آموزش میدهد



- اولین لایه در ارسال اطلاعات کدام لایه است ؟ لایه ۷
- اولین لایه در ارسال اطلاعات کدام لایه است ؟ لایه ۱

لایه ۱ – physical

در این لایه فقط وفقط صفر و یک قابل درک است و دستگاهی مانند Hub،switch ، وتمام تجهیزات شبکه ای قابل لمس لایه یک محسوب میشوند

وسیله ای که صرفا فقط لایه یک محسوب میشود کابل است

لایه ۲ – data link

آدرس دهی مهم ترین کار یک شبکه است چرا که باید بسته ای را با آدرس مبدا و مقصد ارسال کند اگر این آدرس دهی در کار نباشد نمیتوان بسته ای را ارسال کند

آدرس مبدا source address و آدرس مقصد destination address دو شکل دارد : ۱- شکل physical و ۲- شکل logical

در لایه ۲ آدرس دهی فیزیکی رخ میدهد به این آدرس فیزیکی MAC address میگویند که دارای ۴۸ در مبنای ۱۶ نوشته میشود . آدرس مبدا و مقصد در مجموع ۹۶ بیت آدرس فیزیکی هستند

هر کارت شبکه دارای یک mac address منحصربه فرد unci میباشد

۲۴ بیت اول vendor address و ۲۴ بیت دوم product میگویند

برای بدست آوردن mac هر کامپیوتر میتوان از راه های متفاوتی عمل کرد

۱- Ncpa.cpl کارت شبکه مورد نظر را باز میکنیم و با انتخاب گزنیه detail میتوان mac address را مشاهده کرد
۲- درCMD میتوان با دستور ipconfig – all میتوان تمام آدرس های فیزیکی های موجود دریک کامپیوتر(به تعداد کارت شبکه های موجود) مشاهده کرد ipconfig /all
۳- دستور getmac فقط نمایش mac را به عهده دارد و شماره ریجستر شده را نمایش میدهد و نوع سخت افزار را مشخص نمیکند

در سایت macvendors.com میتوان آدرس سازنده را به ما میگوید

برای فهمیدن mac کامپیوتر های متصل میتوان از دستور arp –a استفاده کرد

چه دستگاهی از MAC اطلاع دارد ؟ bridge ، switch

mac table = آدرس های فیزیکی موجود در یک سوئیچ برای آدرس دهی راحتتر و تشخیص آدرس برای رساندن بسته به مقصد

اگر mac table کامل(learn) نشده باشد با اولین بسته ای که به سمت سوئیچ می دهد نگاه به source کرده و آن را learn میکند

اگر mac table قبلا learn نشده باشد یک فایل broad cast ارسال میکند تا دیگر آدرس های فیزیکی را learn کند .

سوئیچ برای هر آدرس فیزیکی یک مدت زمان خاص age در نظر میگیرد

Mac address-table aging time 300 seconds

برای تغییر در زمان نگهداری مک از دستور زیر استفاده میکنیم

Mac address-table aging-time second [**vlan** vlan-id]

انواع ترافیک در شبکه

Unicast – multicast - broadcast

Unicast = ارسال یک به یک –ارتباط مستقیم یک سیستم با یک سیستم دیگر به طور مستقیم

Multi cast = یک به چند – ارتباط یک سیستم با چند سیستم دیگر ، ارسال داده از یک سیستم برای ده سیستم از ۱۰۰ سیستم

Broadcast = یک به همه سیستم های موجود – یک سیستم ارسال کننده داده ها برای تمام سیستم های داخل شبکه

Broad cast domain = محدوده ای که اگر یک سیستم broadcast ارسال کند تمام سیستم های broadcast domain دریافت خواهند کرد

برای محدود کردن broadcast چند راه داریم ۱- subneting ۲- vlan

آدرس های لایه ۲ فیزیکی است توسط کارخانه سازنده generate میشود و سخت افزار با آن کار میکند

آدرس های لایه ۳ logical منطقی هستند

لایه ۳ – NETWORK

مهمترین لایه osi است و آدرس دهی خاص خود را دارد و این آدرس ها ip هستند و logical هستند چرا که خود ما این آدرس ها را تعیین میکنیم و این آدرس گذاری باید انجام شود چرا که بتوان از سرویس های مد نظر استفاده کرد

Ip address –ادرس لایه ۳ - logical address

Ip ها بر مبنای ۱۰ دیسیمال نگارش میشوند و دارای ۳۲ بیت هستند.

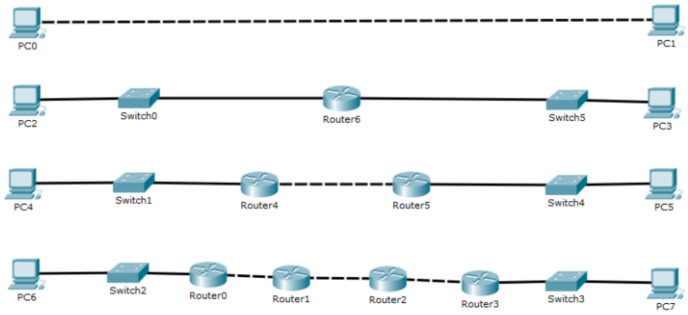
اگر بخواهیم شبکه ای را بسازیم به چه وسیله ای میسازیم ؟ آدرس های IP

چه دستگاه هایی لایه ۳ هستند ؟ دستگاه هایی که IP پذیر هستند router – modem – access point

لایه ۴ – Transport

کامپیوتری هایی که به طور مستقیم در چند حالت با هم در ارتباط هستند.

Host ما ادر نهایت از ابتدا تا لایه چهارم به هم متصل هستند و هم دیگر را میبینند و با هم ارتباط دارند



TCP – UDP

UDP = با سرعت بیشتر و دقت کمتری عمل میکند . "کمیت بهتر"

TCP = با سرعت کمتر و دقت بیشتری عمل میکند و " کیفیت بهتر"

Reliability = اطمینان از بسته ارسال شده ودریافت در مقصد/اگر بسته ای ارسال نشد دوباره سعی خواهد کرد

Establishes, miantains, and terminates virtual circuts = برقراری اتصالی(لایه ۴) از طریق مدار مجازی برای اتصال با چندین مقصد و منابع دیگر ، به وسیله این گزینه برقرار ، نگهداری و تعمیر و قطع میشود لایه ۴ مهم ترین لایه کاربردی در شبکه است

اگر خطایی تشخیص داده شد توسط لایه ۴ شناسایی شده و رفع خطا میگردد و سرعت را sync میکنند

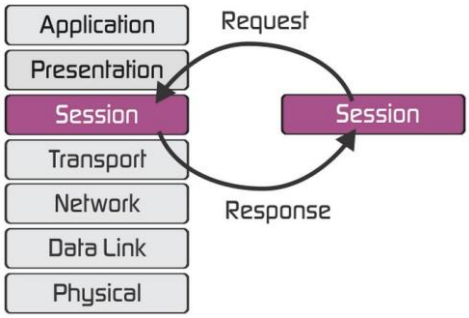
برای اینکه بفهمیم چه host هایی به host من و بلعکس متصل هستن از دستور netstate -n استفاده میکنیم

برای تشکیل یک ارتباط مجازی (virtual circuts) از واژه port استفاده میکند پورت ها ۱۶ بیت هستند که از صفر تا ۶۵۵۳۵ تشکیل میدهد که میتوان با یک host ۶۵۵۳۵ connection به طور همزمان برقرار کرد.

لایه ۵ – Session

ارتباطی موقت بین host ها که باعث میشود نرم افزار ها باهم ارتباط برقرار کنند و این ارتباط را تا زمان مورد نظر برقرار نگه دارند و اینکه یک نرم افزار در یک شبکه با یک نرم افزار دیگر در شبکه با هم در ارتباط باشند یک session تشکیل میدهند مانند chrome و google

میتوان در لایه پنج مدیریت و شروع و پایان یک session را برعهده دارد



لایه ۶ – persentation

باعث میشود که تمام date را readable کنیم

میتوان ارتباط برقرار کرد نوع data و format آن مشخص میشود

داده را فشرده سازی میکند و یک negotiates بین لایه ۶ و ۷ را دارد .

داده را encryption ارسال میکند

در این لایه برقراری ارتباط شبکه ای میان سیستم عامل های مختلف مانند ویندوز ، لینوکس و .... به عهده این لایه است .

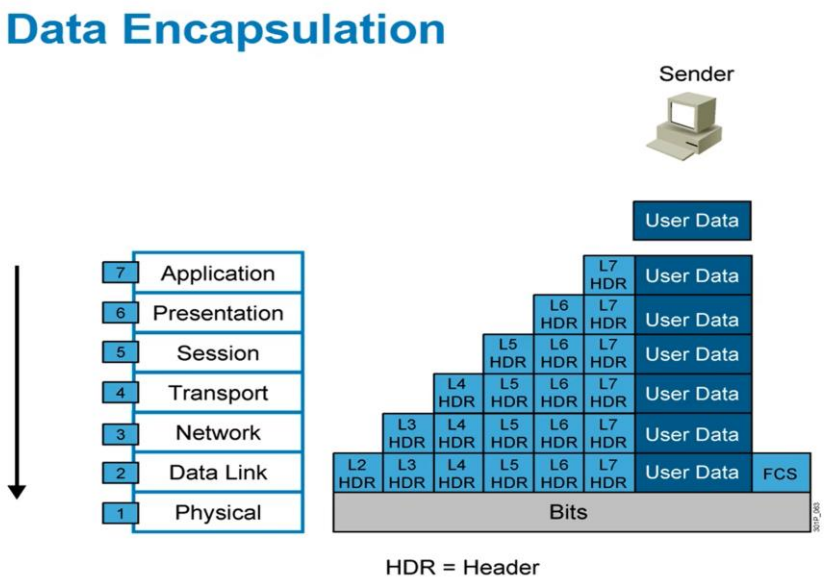
- Cisco دارای سیستم عامل unix است

لایه ۷ – aaplication

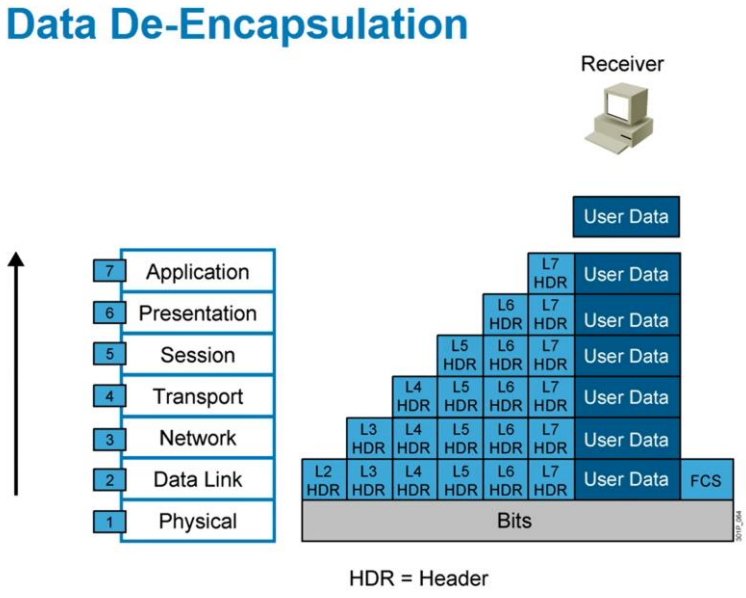
نرم افزار هایی که میتوان از آنها در شبکه بهره برد و و در این لایه network service ها را برای application proccess را فراهم میکند . مانند chrome

در لایه ۷ ارائه دهنده service provider کنترل احراز هویت دارد

وظیفه لایه ۷ = فراهم نمودن سرویس های شبکه ای برای سرویس های مد نظر

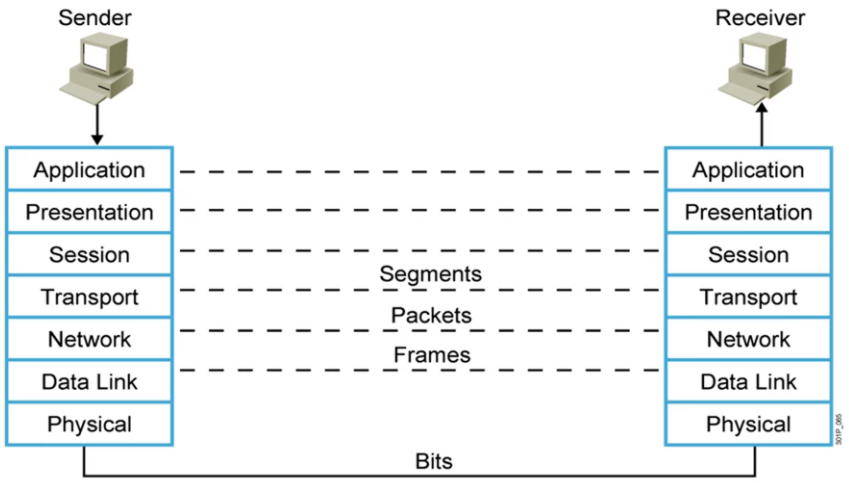


تصویر بالا بازگو کننده این است که Data بخواهد در شبکه ارسال شود هر لایه header خاص خود را به این بسته اضافه میکند و آخرین کسی که header اضافه میکند لایه ۲ است



در مقصد اضافه شده لایه ها را باز میکند و آن را به لایه ۷ میرساند .

Peer-to-Peer Communication



packet data unit = PDU

واحد data ما وقتی یک header به آن اضافه میشود به آن segment میگویند .

pdu لایه ۴ را نام ببرید ؟ segment

PDU واحد Data که دارای header لایه ۳ باشد نام ببرید ؟ packet

PDU واحد Data که دارای header لایه ۲ باشد نام ببرید ؟ frames

در لایه ۴ علاوه بر segment نوع آن و پروتکل TCP /UDP و پورت به بسته اضافه میشود.

در لایه ۳ علاوه بر packet source ip و destination ip به بسته اضافه میشود.

در لایه ۲ علاوه بر frames source mac و destination mac به بسته اضافه میشود.

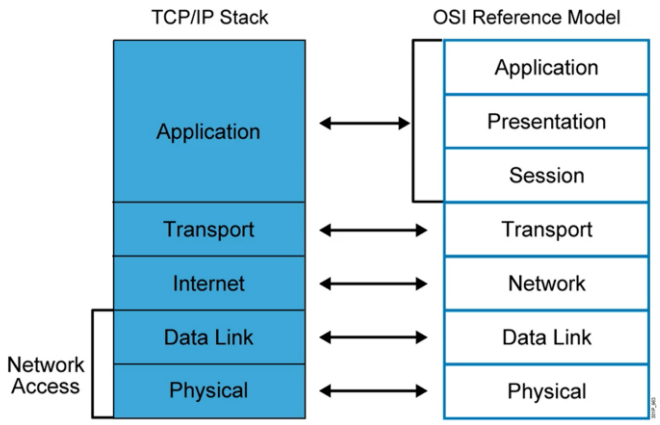
Stack protocol = یک سری پروتکل هایی که جمع آوری شده اند تا یک پروتکل واحد بسازند اگر مجموعه ای پروتکل داشته باشیم که در مجموع یک کار واحد را انجام دهند به آن stack پروتکل میگویند .

TCP/IP

مجموعه از پورتکل ها که یک کار واحد را انجام میدهد و آن ارتباطات شبکه ای است و soucrce open میباشد

چرا tcp/ip روی همه پلتفرم ها وجود دارد ؟ بخاطر وجود شبکه جهانی اینترنت

TCP/IP Stack vs. the OSI Model



Ip addressing

Ip classfull

X.X.X.X **32 bite** **in decimal format**

Class A : 1 – 126

Class B : 128 - 191

Class C : 192 - 223

Class D : 224 – 235 (MULTI CASTING)

Class E : 236 - 255 (RESERVED FOR RESEARCH)

کلاس های A , B, C را به اسم UNICAST PUBLIC AND PRIVTE ADDRESS می گویند.

SUBNETMASK

هر IP یک SUBNETMASK دارد و هر بخش (OCTED IP) (هر بازه ۸ تایی) یک بخش متناظر دارد که به آن SUBNETMASK میگویند که نشان دهنده بازه تغیرات کلاس IP می باشد و میتوان با IP و SUBNET MASK شبکه های مجزایی را ساخت . مقدار sUBNET MASK صفر یا ۲۵۵ است

IP address	X. X. X. X
Subnet mask	Z. Z. Z. Z (by default Z is 0 or 255)

IP ها دو حالت دارند : ۱- CLASS FULL ۲- CLASS LESS

Class A : 1 – 126 SUBNETMASK = 255.0.0.0

Class B : 128 - 191 SUBNETMASK = 255.255.0.0

Class C : 192 - 223 SUBNETMASK = 255. 255. 255.0

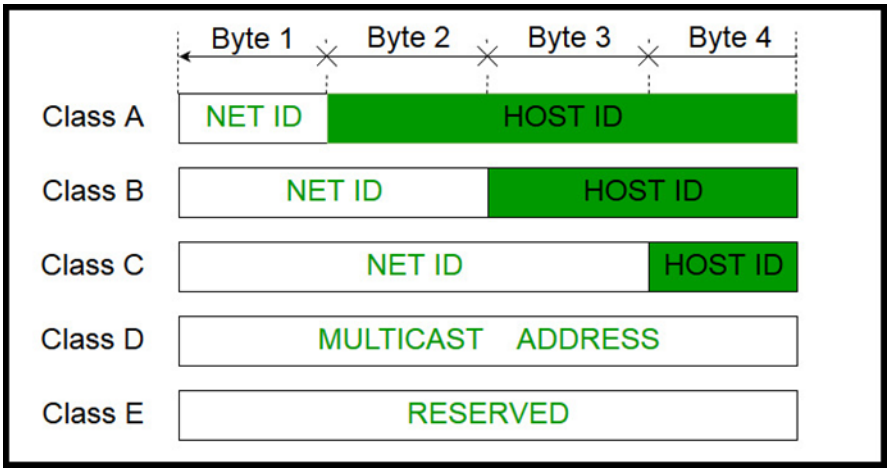
۲^۲۴=۱۶,۷۷۷,۲۱۶ -۲

۲^۱۶=۶۵,۵۳۶ -۲

۲^۸=۲۵۶ -۲

اولین IP و آخرین IP رزرو می باشد چرا که IP اول PARENT و IP آخر BROADCAST نام دارد .

اولین IP برای معرفی شبکه است و آخرین IP رزرو برای ارسال یک بسته به کل شبکه است .



PUBLIC AND PRIVATE IPs

وقتی ip ها را تقسیم میکنیم به دو دسته کلی تقسیم میشود

Ip هایی public است که در اینترنت استفاده میشود و قابل دسترسی است

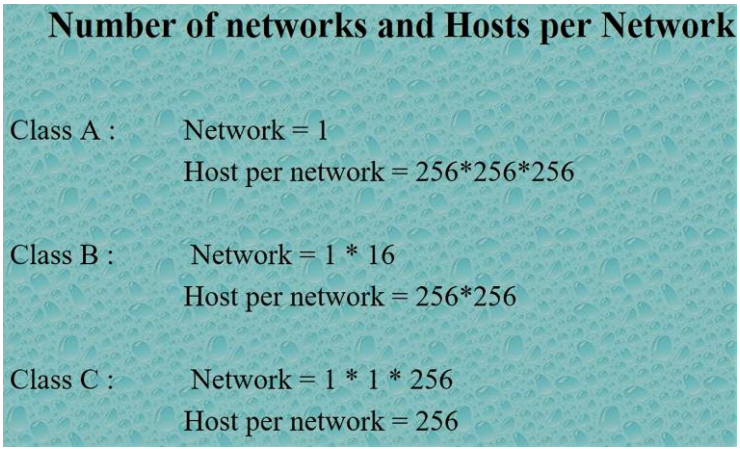
Ip هایی private است که در یک شبکه داخلی استفاده می شود و در اینترنت قابل استفاده نیست

Ip class less

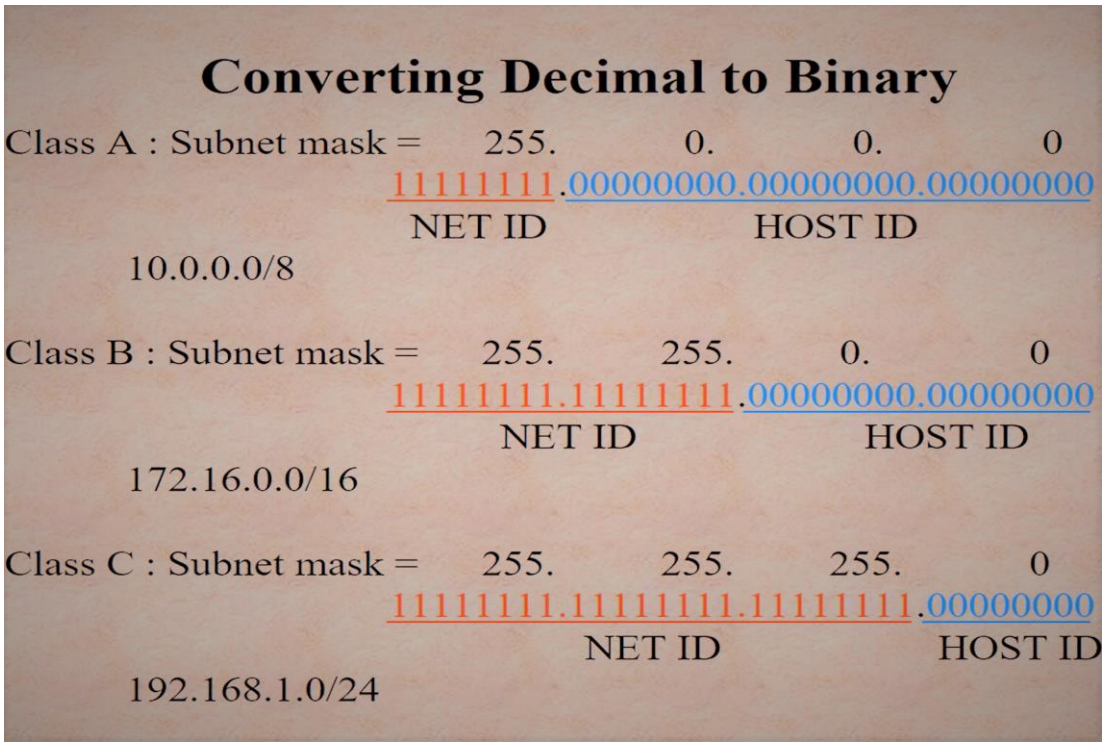
VLSM= variable length subnet mask

برای اینکه بخواهیم تعداد host های بیشتری داشته باشیم میتوانم از روش class full استفاده کنیم

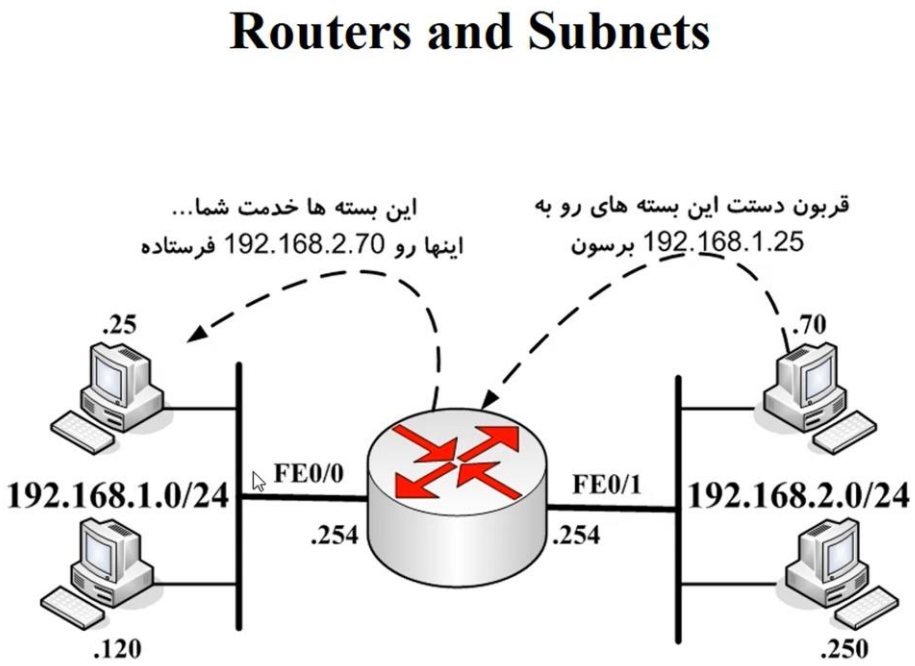
به همین دلیل subet mask را از حالت default خارج میکنیم .



Prefix = تعداد بیت های یک باینری یک subnetmask است . پس برای هر مقدار subnet mask که تعداد بیت های آن یک می باشد یک prefix درنظر میگیریم مانند تصویر



تصویر زیر بازگو کننده اتصال دو شبکه مجزا است که ip آن به صورت parent نمایش داده شده و بجای Subnetmask از prefix در آن استفاده شده است.



برای اتصال دو شبکه مجزا از یک device به نام router استفاده میکنیم .پس باید یک ip از شبکه مورد نظر را بر روی interface مسیریاب قرار دهیم

یک router به تعداد interface هایی که دارد میتواند شبکه های مجرا به هم متصل کرد و برای اینکه پورت های یک router را بشناسیم بر روی interface router با نام های E و F و G مشخص شده است .

G=gigABITETHERNET F=FASTETHERNET E= ETHERNET

هر host برای رسیدن به router و شبکه مجزا نیاز به راه خروج (GETWAY) دارد

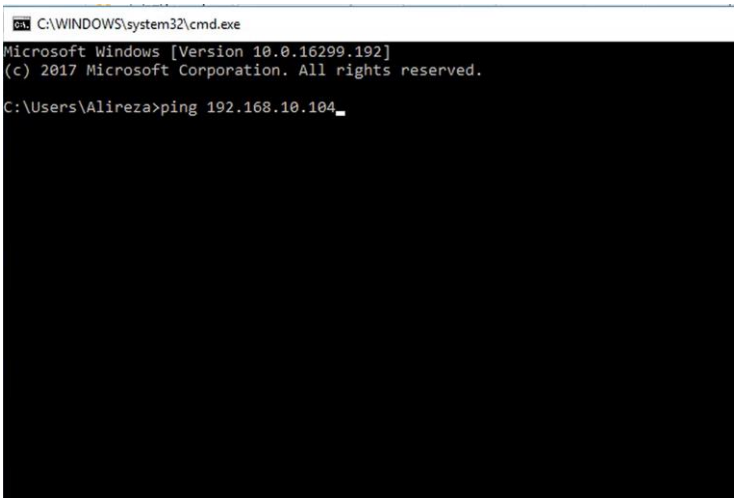
ICMP= INTERNET CONTROL MANAGEMENT PROTOCOL

وظیفه چک کردن اتصال شبکه را دارد . میتوان یکی از مهم ترین ابزار های ICMO را PING دانست

با این ابزار میتوان از لایه ۱ تا لایه ۳ چک کردن و از سلامت آنها اطمینان کسب کرد .لایه ۱= کابل و کابل کشی

لایه ۲ = MAC ADDRESS ها

لایه ۳ = میتوان فهمید که IP ها سالم و DEVICE ها همدیگر را میبینند

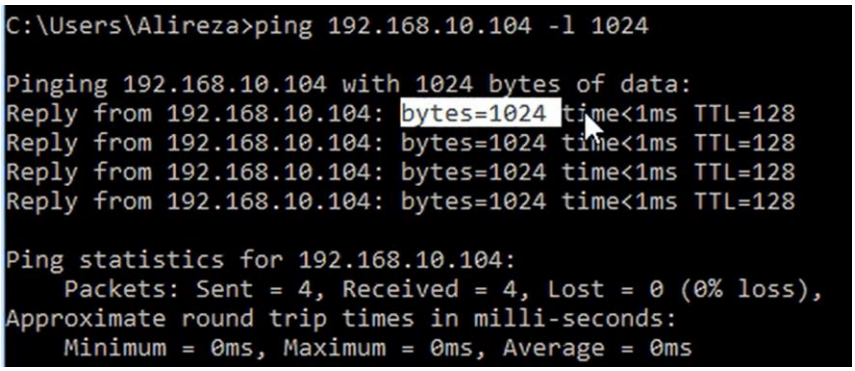


ازابزار PING برای چک کردن یک ارتباط به کار میرود ، خروجی دستور مطالب زیادی را به اطلاع ما می رساند

درخواست ما را ارسال میکند(ICMP REQUEST (ECHO REQUEST

و IP مورد نظر به ما پاسخ میدهد ICMP REPLAY و میتوان با تغییر دستور مقدار بسته ارسالی ICMP را تغیر داد

>PING 192.168.10.100 –L 1024



TIME TO LIVE =TTL

مشخص کننده نوع سیستم عامل هم نیز میتواند باشد

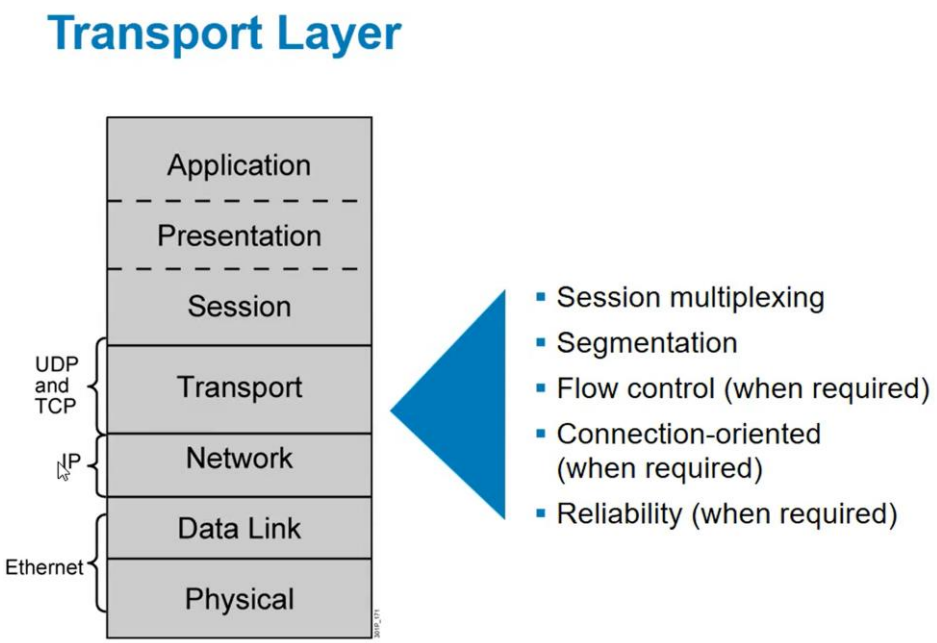
TTL=128 سیستم عمال مایکروسافت / TTL=64 لینوکس

اگر بخواهیم بفهمیم که بین HOST من و یک سایت چند DEVICE وجودوجود دارد از دستور TRACERT استفاده میکنیم

TRACERT GOOGLE.COM –T

لایه ۴- TCP/IP

مدل OSI همان TCP/ip است



ETHERNET

یک پروتکل لایه یک و دو هست که وظیفه انتقال بسته ها بر روی سیم مسی است .

ethernet در لایه ۲ عمل میکند که source mac و destination mac را به روی بسته میگذارد و وظایف لایه ۲ را انجام میدهد (۱۰-۱۰۰ Mb ethernet)

Ip وظایف لایه ۳ را انجام میدهد

وظایف لایه ۴ –Trancprot

وظیفه لایه ۴ انتقال بسته ها است اگر لایه ۴ نبود به طور همزمان یک کار در شبکه نمیتوان انجام داد.تقسیم بندی (segment) یکی دیگر از وظایف این لایه است

Flow control = تنظیم سرعت شبکه و کارت شبکه های متصل به شبکه

TCP&UDP

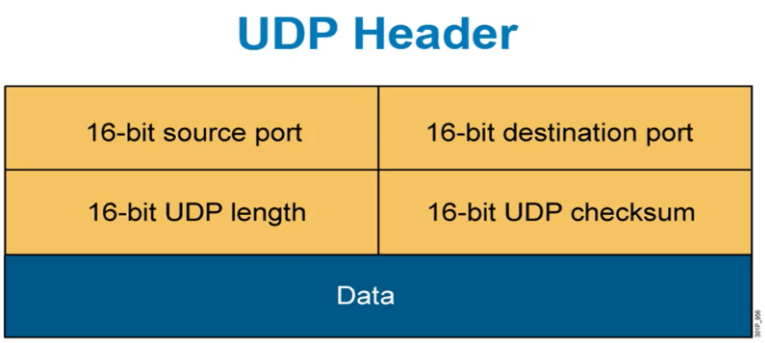
UDP= سریعتر – قابلیت اطمینان کمتر بدون ماکان بازیابی – **بدون** ترتیب ارسال بسته (BEST-EFORT)

خصوصیات

- در لایه TRANCPROT OSI , TCP/IP کار میکند
- دسترسی APPLICATION به لایه شبکه (NETWORK)بدون RELAYBELITY
- CONNECTIONLESS PROTOCOL
- محدودیت در کشف خطا ERROR CHECKING
- کمیت بسیار خوب BEST – EFFORT DELIVERY
- بازیابی ندارد NO DATA RECOVERY

HEADER های زیر به بسته UDP اضافه میشود این مقادیر به عنوان HEADER لایه ۴ اضافه میشوند از همه مهم تر SOURCE PROT و DESTINATION PORT می باشد

در مقصد DESTINATION PORT یک پورت سرویس دهنده است.(WEB SERVER)



سربار HEADER UDP - ۶۴ بیت

ترکیب IP و PORT =SOKECT

در UDP کنترل خاصی روی ارسال بسته ندارد و ارسال میکند اما TCP در مقصد به HOST مقصد اعلام آمادگی میکندو بسته ارسالی را اعلام میکند تا HOST امکان دریافت بسته را قبول کند.

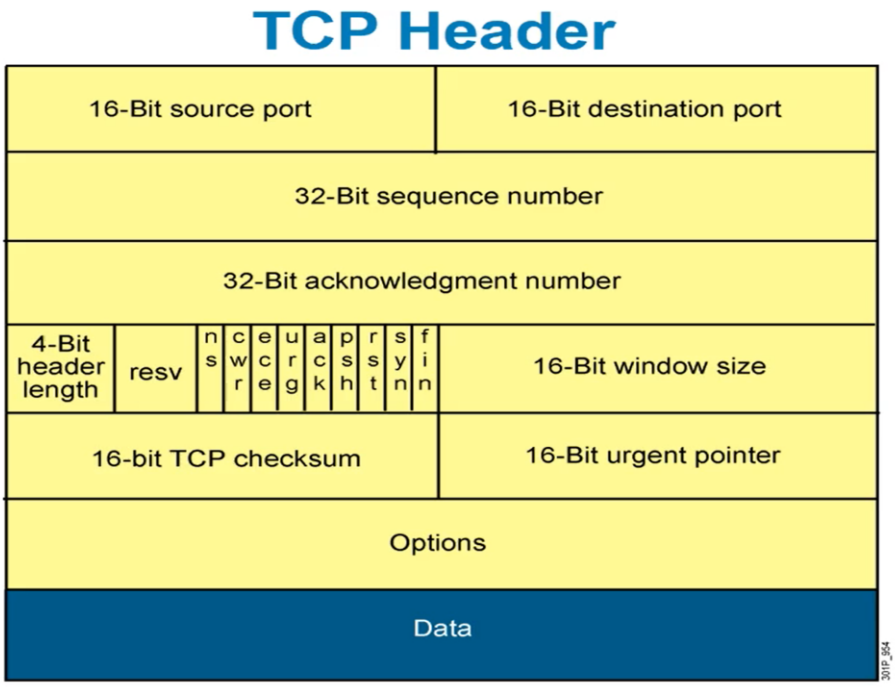
Connection – oriented =پس از آمادگی دریافت بسته در نقصد یک CONNECTION برقرار کرده و بسته های مورد نظر را ارسال میکند و پس از پایان ارسال بسته ها این CONNECTION را قطع میکند

TCP = کندتر – دقت بیشتر ، اطمینان پذیری بالاتر - **با** ترتیب ارسال بسته (RELAYBILITY)

- متفاوت در CONNECTIONORIENTED بودن
- Miss packet recovery

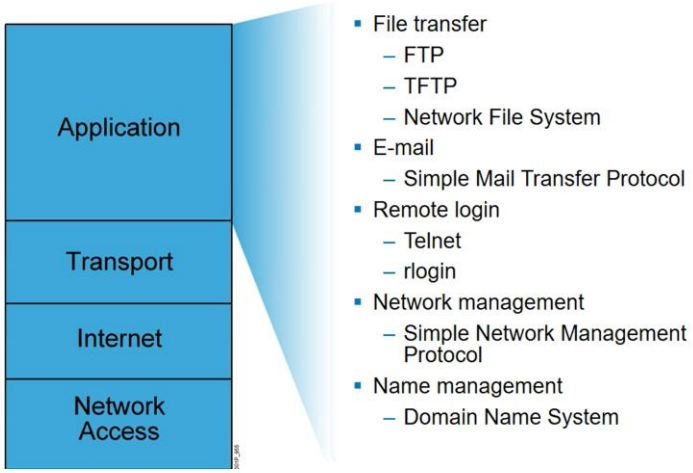
خصوصیات

- کار در لایه TRANCPROT
- دسترسی دادن APPLICATION به NETOWRK
- CONNECTION ORIENTED
- FULL-DUPLEX ایجاد cONNECTION های متفاوت برای اتصال به چند نقطه مختلف
- ERROR CHECKING
- SEQUENCING PACKET
- ACKNOWLEDGEMENTOF RECEIPT
- DATA RECOVERY FEATURES

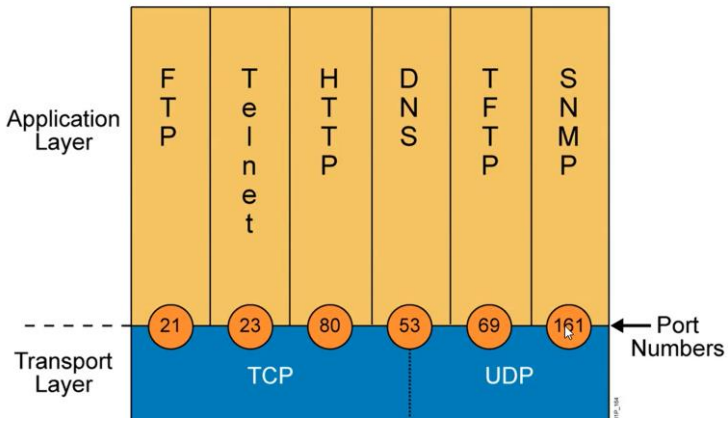


سربار HEADER TCP ۱۹۲ بیت

TCP/IP Application Layer Overview



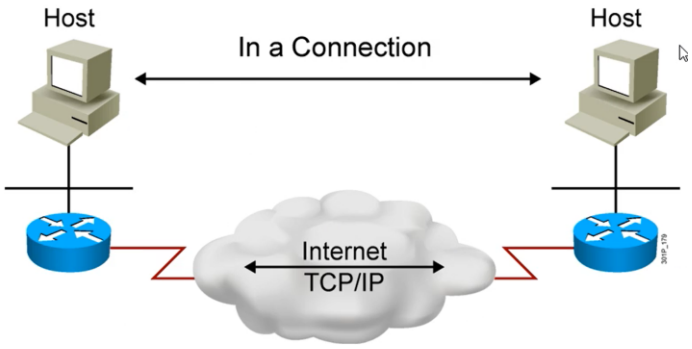
Mapping Layer 4 to Applications

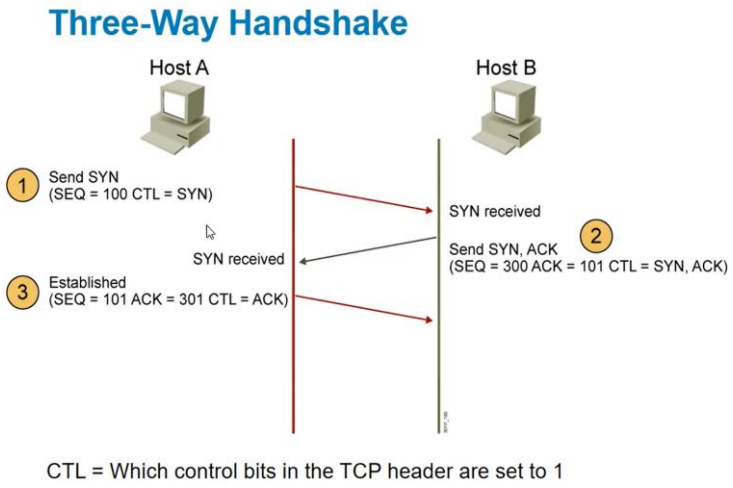


THREE-WAY HAND SHAKE

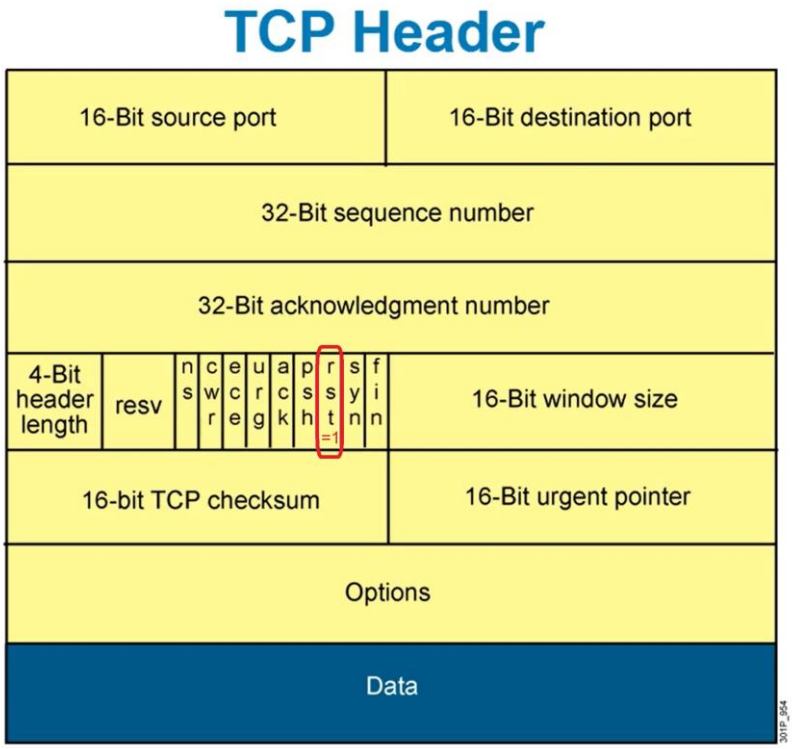
براقرار کننده CONNECTION قبل از ارسال

Establishing a Connection





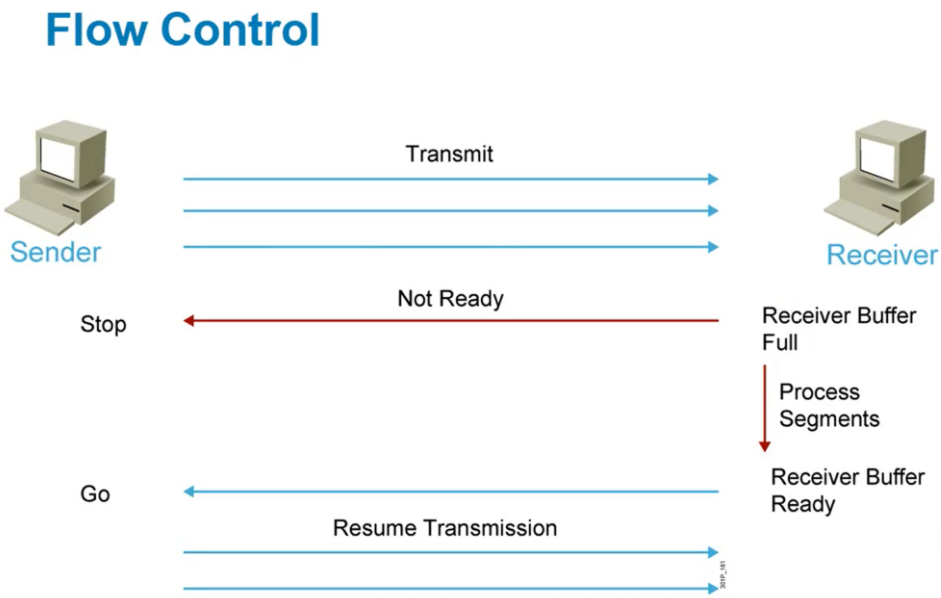
اگر یک HOST ظرفیت پذیرش یک بسته را نداشته باشد برای فرستنده CTL – RST را به مقدار یک باز میگرداند.



SYN FLOOD حمله ای تحت شبکه برای برقراری ارتباط

FLOWCONTROL

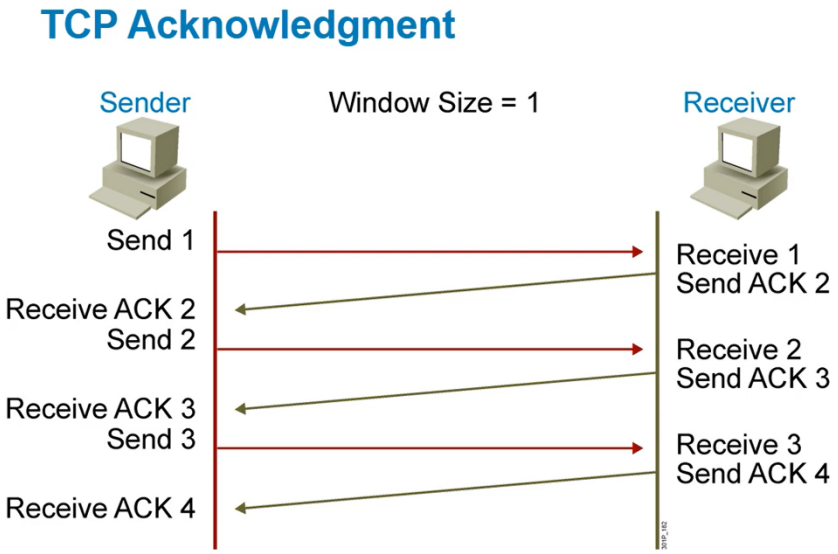
هنگامی که یک ارسال کننده و یک دریافت کننده دارای ارتباط باشند و دریافت کننده سرعت کمتری داشته باشد پس قطعا BUFFER آن سریع تر تکمیل خواهد شد و برای ارسال کننده پیامی ارسال میکند تا ارسال بسته را متوقف کند و وقتی که پردازش تمام شد بسته درخواست ادامه ارسال را به فرستنده میفرستد تا ارسال بسته ها ادامه یابد



نکته FLOW CONTROL سرعت ما را به صورت سخت افزاری کاهش نمی دهد .

ACKNOWLEDGEMENT

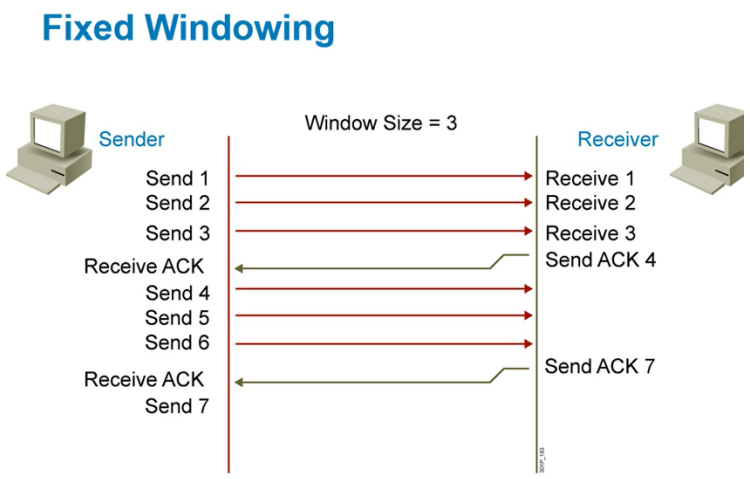
ACKNOWLEDGEMENT تعین میکند که هر تعداد بسته مشخص شده DELIVERY ارسال کند.



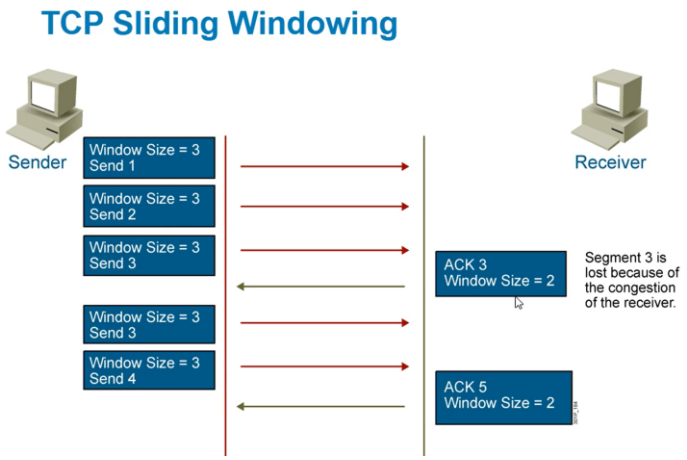
با تعیین شدن WINDOWS SIZE پس از ارسال و دریافت از HOST گیرنده علاوه بر DELIVERY شماره ACK بعدی را ارسال میکند تا بسته ها به ترتیب ارسال و دریافت شوند.

به توجه به تصویر دریافت کننده بسته ۱ را دریافت کرده و در جواب SEND ACK 2 را به فرستنده ارسال مبکند تا بسته بعدی ارسال شود و اگر بسته ای به طور کامل دریافت نشود مجددا SEND ACK 1 را ارسال میکند تا بسته دریافت شود و HOST فرستنده از روی شماره ACK متوجه دریافت بسته میشود.

✓ اگر WINDOWS SIZE دارای حجم کم باشد ترافیک بسیار بالایی را در شبکه ایجاد میکند چرا که پس از هر دیافت باید رسید بازگرداند . اگر WINDOWS SIZE را ۳ قرار دهیم هر ۳ بسته پیام رسید دریافت میشود طبق تصویر زیر

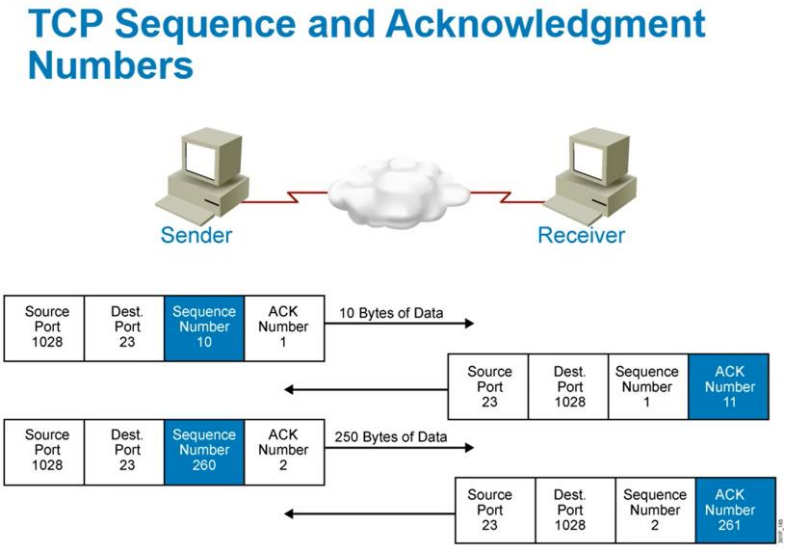


اگر بسته ای در راه MISS شود شماره ACK را مقدار بسته MISS شده میگذارد تا بسته دوباره ارسال شود و مقدار WINDOWS SIZE هم کاهش میدهد تا داده ها کامل دریافت شوند.



از روی HEADER بسته میتوان به این درک رسید که این بسته از کجا می آید و مقصد آن کجاست

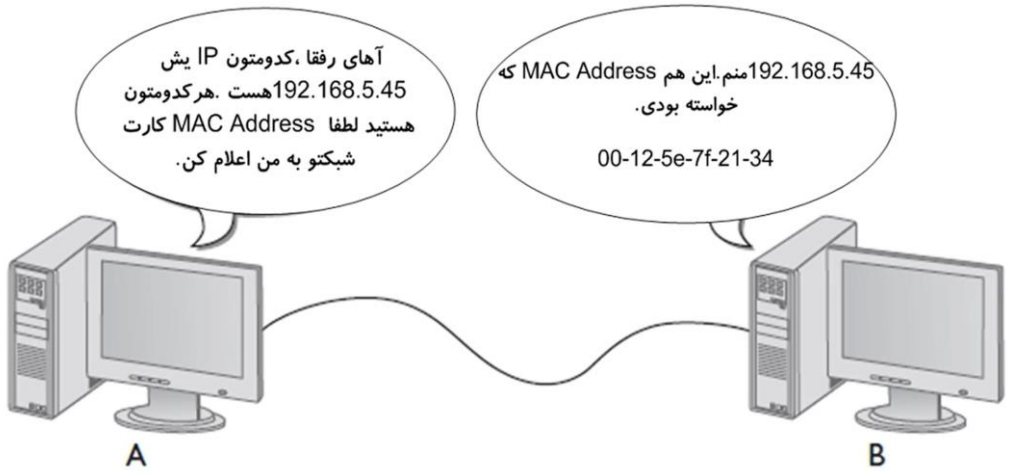
از کجا آمده ام ، به کجا میروم ، آمدنم بهر چیست ؟



ARP – ADDRESS RESOLUTION PROTOCOL

اگر بسته ای بخواهد از HOST A به HOST B دیگر ارسال شود آدرس مبدا SOURCE IP فرستنده قرار میگیرد و DESTINATION IP در لایه۳ مشخص میگردد و PACKET میشود و هنگامی که در لایه ۲ FREAM ساخته شود SOURCE MAC را میداند ولی DESTINATION MAC ندارد.

بنابراین بسته PARK شده و تاهنگامی که HOST B بفهمد MAC مقصد چیست!! این کار به وسیله ARP PROTOCOL انجام میشود .



HOST B صرفا پاسخگو نیست و MAC HOST A را در جدول خود نوشته و سپس پاسخ میدهد تا در فرستادن ARP صرفه جویی کندو پس از دریافت پاسخ توسط HOST A و ارسال بسته MAC HOST B هم در جدول HOST A ذخیره میشود.

محل ذخیره این جدول در ویندوز در خط فرمان CMD و با دستور arp –a قابل مشاهده است.

نکته : این جدول همیشه خالی است و حافظه arp پاک میشود و پس از برقراری ارتباط باشبکه تکمیل میشود چرا که پس از اتصال به شبکه باید یک arp broad cast در شبکه ارسال شود و **به همین دلیل میگویند هزار کامپیوتر را دریک شبکه قرار ندهید.**

Arp هم دارای age می باشد.

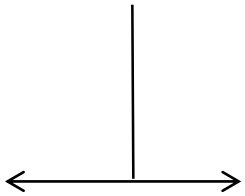
درجدول ARP واژه DYNAMIC بودن به معنای دریافت MAC از راه BROAD CAST است

```
C:\Users\Tarahan>arp -a

Interface: 192.168.199.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.199.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.47.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.47.254        00-50-56-fd-d8-ac     dynamic
  192.168.47.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

نماد زیر نشان دهنده broad cast در شبکه است .

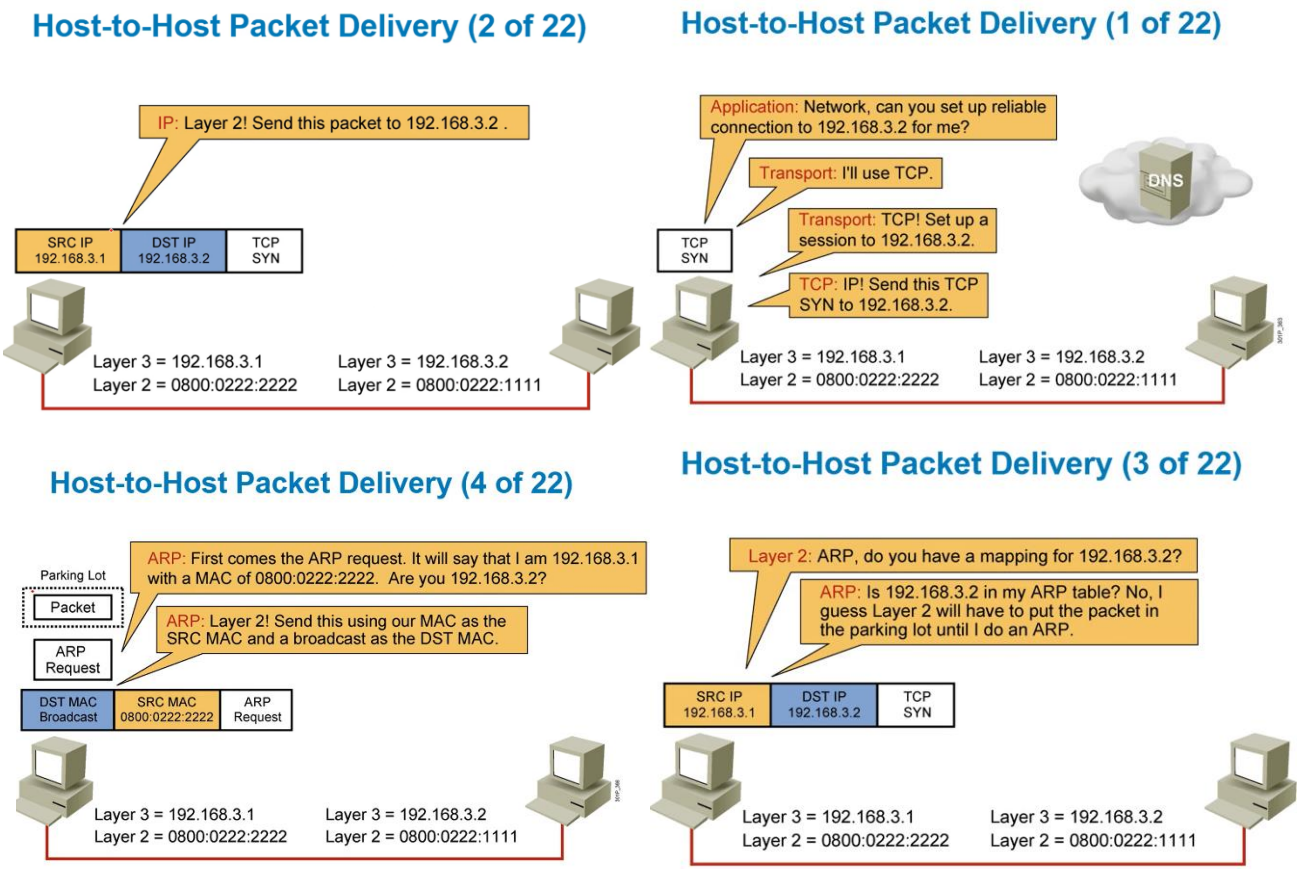


اگر DESTINATION MAC ۴۸ بیت یک داشته باشد (FF:FF:FF:FF:FF:FF) این MAC برای BROAD CAST خواهد بود و برای همه در شبکه ارسال خواهد شد .

ارسال بسته در شبکه

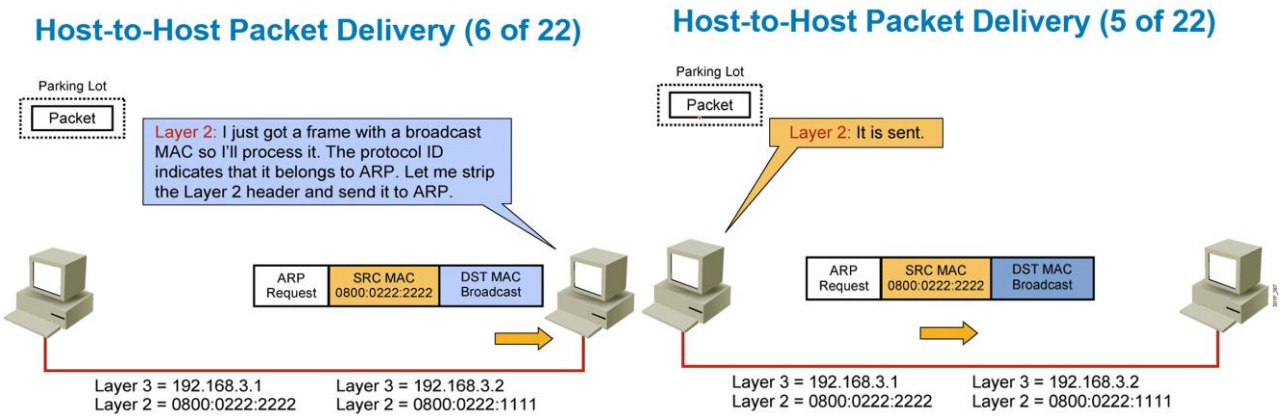
LAYER2 = MAC ADDRESS

LAYER 3 = IP ADDRESS

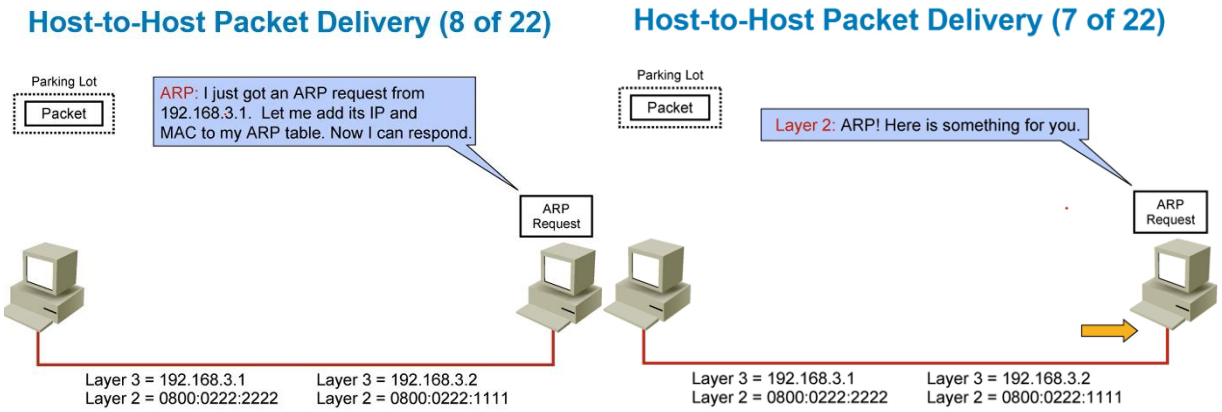


در تصویر ۳ لایه ۲ از ARP سوال میکند که آیا MAP انجام داده ای ؟

ARP در جدول خود نگاه کرده و اگر نباشد به ارسال کننده بسته میگوید که بسته را پارک کن تا پیام BRAODCAST را ارسال کنم و پاسخ دهم و به جای بسته data بسته ای با نام arp request ساخته شده و در شبکه ارسال میشود و از اعضای شبکه سوال میشود(broadcast) که میگوید مبدا ۳,۱ هستم و ۳,۲ کیست ؟ و لایه ۲ فریم arp ارسال میکند

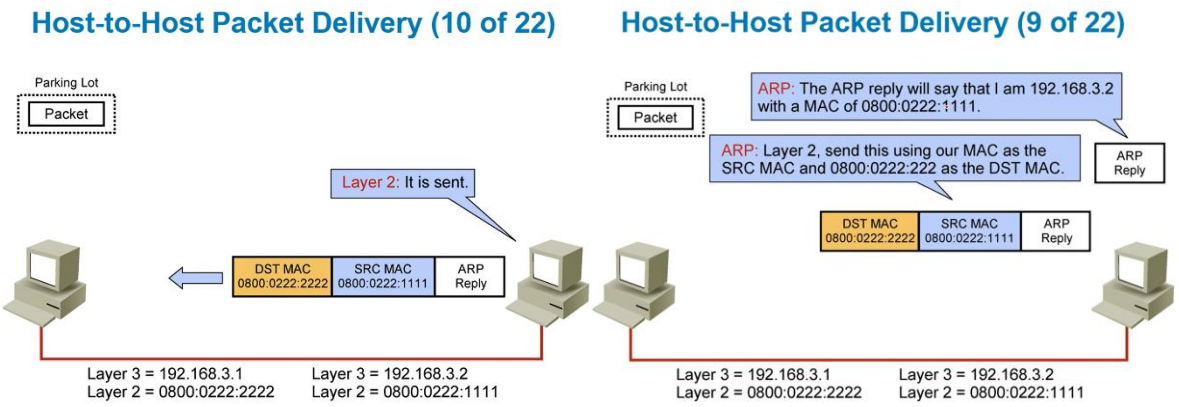


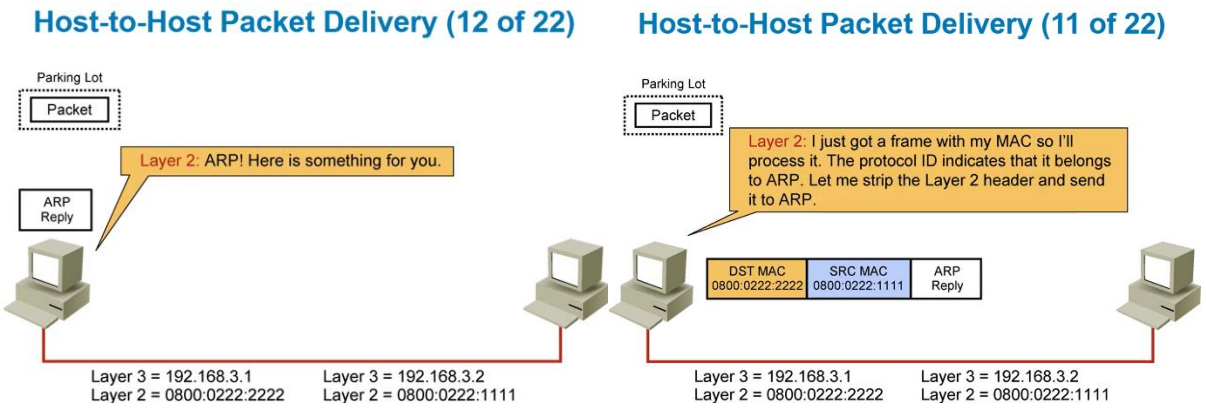
هنگامی که بسته توسط لایه ۲ دریافت شد میگوید یک فریم از نوع broadcast دریافت کردم که باید پردازش شود سپس header layer2 جداسازی شده و بخش Arp request را برای arp ارسال میکند.



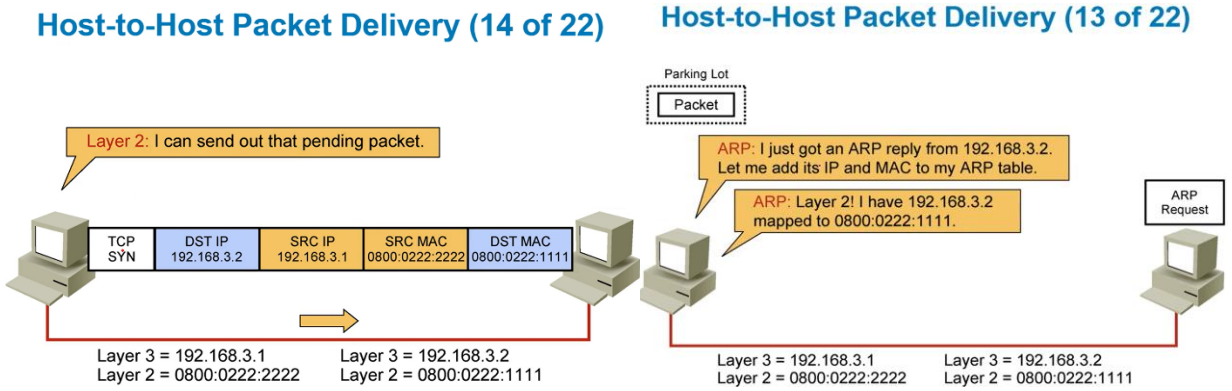
بسته دریافت شده از طریق arp در host B را که حاوی MAC و ip host A می باشد ذخیره میکندو پس از ان پاسخ میدهد واز لایه ۲ میخواهد که بسته را ارسال کند و دربسته source mac و destination mac از نوع unicast به host A ارسال میکند

نکته : هنگام برگشت arp replay به طور unicast ارسال میشود چرا که source mac و destination mac را درلیست خود دارد

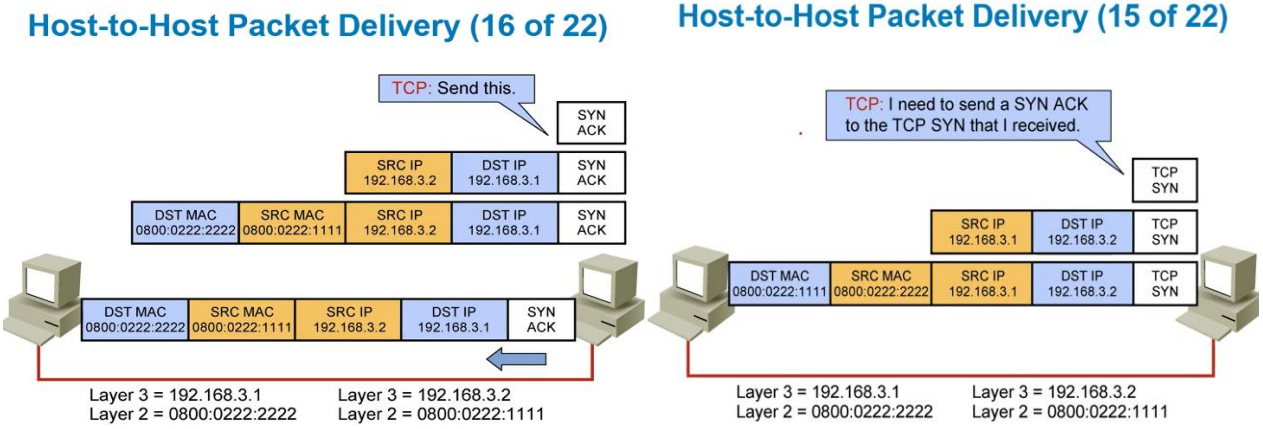




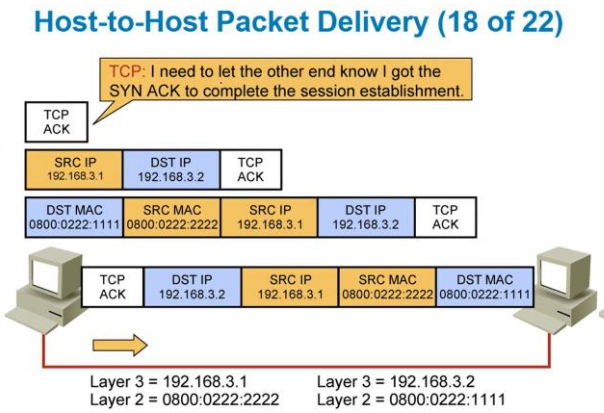
Broadcast زیاد در شبکه باعث میشود تا host های یک شبکه آن را دریافت کنند و به پردازش آن بپردازند و آن را پردازش کنند تا بفهمد برای آنها ارسال شده است یا خیر و سپس عمل resive یا drop کنند

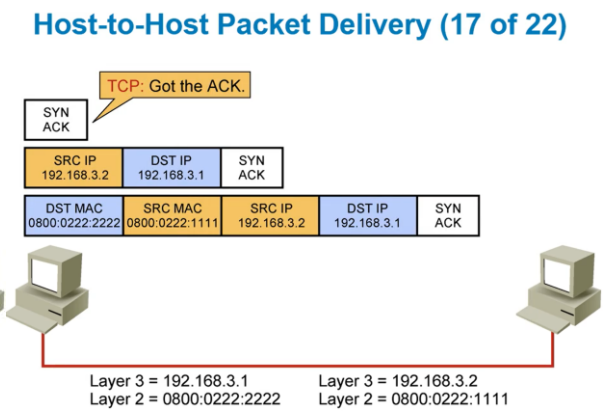


Arp replay را ارسال میکند و به لایه ۲ میگوید که آدرس map شده ر بارگذاری کن و packet park شده را با source mac و destination mac و ip source و ip destination که destination mac را که به واسطه Arp بدست آوردی ارسال کن .



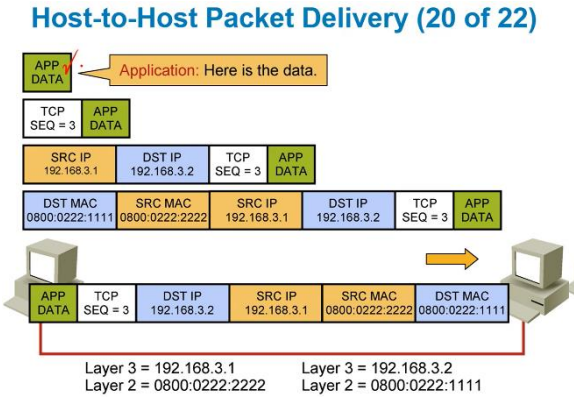
پس از جداسازی لایه های ۲ و ۳ و رسیدن به header لایه ۴ بسته (TCP SYN) را دریافت میکند و پس از آن با SYN ACK پاسخ میدهد به این عمل THREE-WAY HAND SHAKE میگویند

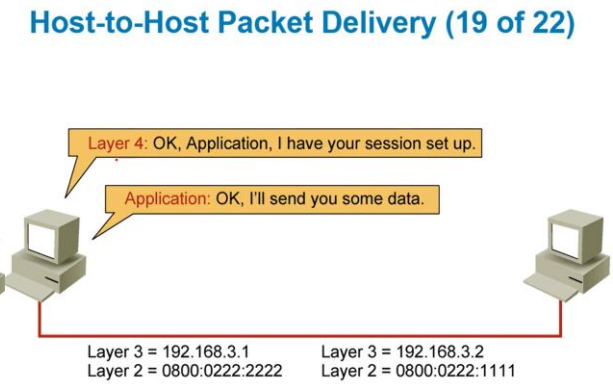




در این مرحله برای کامل شدن SEDDION ESTABLISHMENT با یک جواب SYN ACK به واسطه ساخت یک بسته با چسباندن HEADER لایه ۲ و لایه ۳ و در شبکه ارسال میکند.

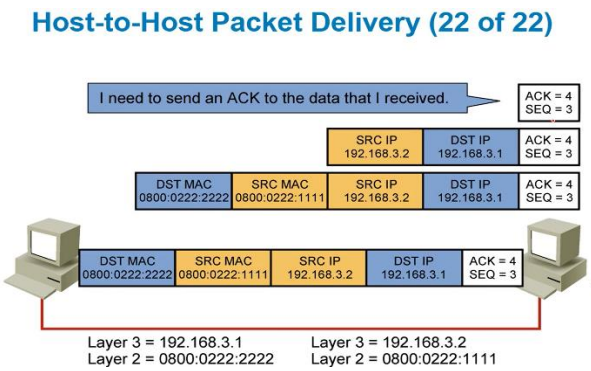
تمام این فرایندها پس از دریافت SOURCE MAC و DISTINATION MAC به طور UNICAST انجام میشود.

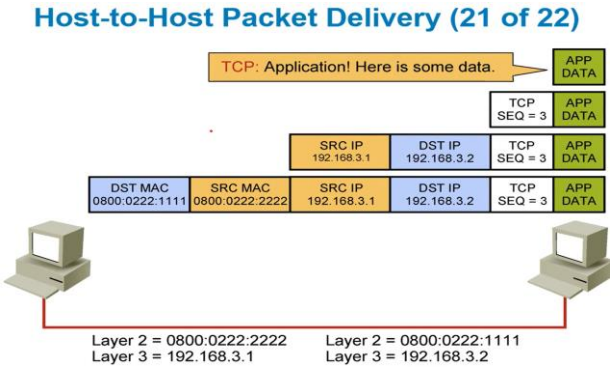




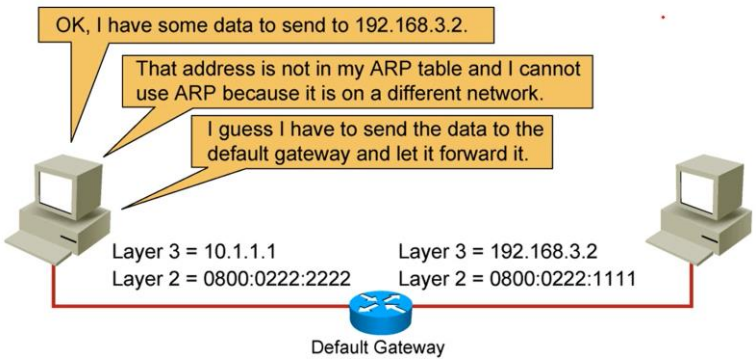
هنگامی که CONNECTION برقرار و بسته ارسال شد درخواست SESSION را برای HOST B SET UP کردم حال برنامه درخواست کننده این ارتباط DATA خود را ارسال میکند.

از لایه ۷ DATA ایجاد شده و در لایه ۴، هدر لایه ۴ SEGMENT و در لایه ۳، هدر لایه ۳ PACKET و در لایه ۲، هدر لایه ۲ FREAM ایجاد شده و برای مقصد ارسال میشود تا کار انتقال DATA به پایان برسد و گزینه FIN را ارسال میکنیم





Default Gateway



اگر بسته ای را بخواهیم از HOST A به HOST B در شبکه ای دیگر بفرستیم باید از GETWAY استفاده کنیم که در تصویر گفته شده برای ارسال بسته آدرس متفاوتی دارند باید ROUTER ارتباط برقرار کند چراکه DATA نمیتوان ارسال کرد به این علت که در شبکه متفاوتی قرار دارد (در BROADCAST شبکه نیست) پس باید DATA از طریق ROUTER یا GETWAY ارسال شود.

پیش فرض age arp ۵ دقیقه است .

END