بیتهای [پرچم](https://fa.wikipedia.org/wiki/%D9%BE%D8%B1%DA%86%D9%85" \o "پرچم): • بیت URG: در صورتی که در این بیت عدد ۱ قرار گیرد معین می‌شود که در فیلد Urgent Pointer مقدار قابل معتبری قرار دارد و بایستی مورد پردازش قرار گیرد. • بیت [ACK](https://fa.wikipedia.org/w/index.php?title=ACK&action=edit&redlink=1" \o "ACK (صفحه وجود ندارد)): اگر در این بیت عدد ۱ قرار داشته باشد به این معنا است که در فیلد Acknowledgment number عدد معتبری قرار دارد. بیتهای ACKو SYN نقش دیگری نیز دارند که در ادامه بدان اشاره خواهد شد. • بیتPSH: اگر این بیت مقدار ۱ قرار گرفته باشد از گیرنده تقاضا می‌شود که داده‌های موجود را بافر نکرده و در اسرع وقت تحویل برنامه کاربردی صاحب آن شود. • بیت RST: اگر در این بیت عدد ۱ قرار گرفته شود به این معنی است که این ارتباط به صورت یک طرفه خاتمه یافته‌است. • بیت SYN: این بیت نقش اساسی در ارتباط یک بسته TCP بازی می‌کند. برقراری ارتباط یک طرفه TCP از روند زیر تبعیت می‌کند • شروع کننده ارتباط یک بستهTCP بدون هیچ داده‌ای و با تنظیم بیتهای ۱= SYN و ACK=۰ تقاضای یک ارتباط جدید می‌کند • در صورتی که طرف مقابل تمایل به بر قراری ارتباط داشته باشد برای طرف مقابل یک بسته با قرار دادن بیتهای ۱= [SYN](https://fa.wikipedia.org/w/index.php?title=SYN&action=edit&redlink=1) و [ACK](https://fa.wikipedia.org/w/index.php?title=ACK&action=edit&redlink=1" \o "ACK (صفحه وجود ندارد))=۱ تمایل خود را برای برقراری ارتباط به طرف مقابل اعلام می‌کند • بیت FIN: اگر یکی از طرفین هیچ داده دیگری برای فرستادن نداشته باشد این بیت را در آخرین بسته برابر ۱ قرار می‌دهد و ارتباط را یک طرفه قطع می‌کند باید توجه داشته که ارتباط هنوز به طور کامل قطع نشده‌است و باید طرف مقابل نیز در آخرین بسته خود این فیلد را برابر ۱ قرار داده تا ارتباط کامل قطع شود.

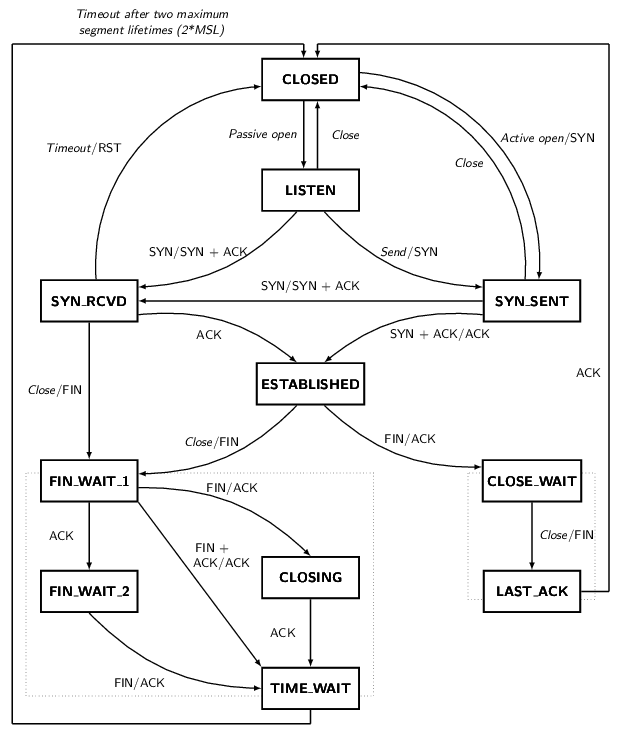
TCP 3-Way Handshake Diagram

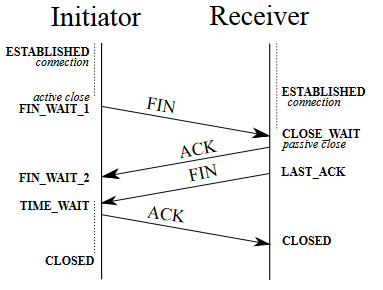
Below is a (very) simplified diagram of the TCP 3-way handshake process. Have a look at the diagram on the right as you examine the list of events on the left.

|  |  |
| --- | --- |
| EVENT | DIAGRAM |
| Host A sends a TCP SYNchronize packet to Host B  Host B receives A's SYN  Host B sends a SYNchronize-ACKnowledgement  Host A receives B's SYN-ACK  Host A sends ACKnowledge  Host B receives ACK.  TCP socket connection is ESTABLISHED. | tcp three-way handshake,syn,syn-ack,ack TCP Three Way Handshake (SYN,SYN-ACK,ACK) |

اگر پروسس tcp از سمت سرور kill شود وضعیت کانکشن در سمت کلاینت close\_wait می شود و تا زمانی که پروسس درخواست ایجاد ارتباط در سمت خود کلاینت قطع نشود در این همین وضعیت باقی می ماند. و در سمت سرور ابتدا به حالت fin\_wait2 می رود و بعد از ان بسته می شود.

اگر پروسس tcp در سمت خود کلاینت kill شود به وضعت time\_wait می رود تا زمانی که در پارامتر مربوطه ست شده باشد.( net.ipv4.tcp\_fin\_timout=30)





LISTEN

(server) represents waiting for a connection request from any remote TCP and port.

SYN-SENT

(client) represents waiting for a matching connection request after having sent a connection request.

SYN-RECEIVED

(server) represents waiting for a confirming connection request acknowledgment after having both received and sent a connection request.

ESTABLISHED

(both server and client) represents an open connection, data received can be delivered to the user. The normal state for the data transfer phase of the connection.

FIN-WAIT-1

(both server and client) represents waiting for a connection termination request from the remote TCP, or an acknowledgment of the connection termination request previously sent.

FIN-WAIT-2

(both server and client) represents waiting for a connection termination request from the remote TCP.

CLOSE-WAIT

(both server and client) represents waiting for a connection termination request from the local user.

CLOSING

(both server and client) represents waiting for a connection termination request acknowledgment from the remote TCP.

LAST-ACK

(both server and client) represents waiting for an acknowledgment of the connection termination request previously sent to the remote TCP (which includes an acknowledgment of its connection termination request).

TIME-WAIT

(either server or client) represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request. [According to [RFC 793](https://tools.ietf.org/html/rfc793) a connection can stay in TIME-WAIT for a maximum of four minutes known as two [MSL](https://en.wikipedia.org/wiki/Maximum_Segment_Lifetime) (maximum segment lifetime).]

CLOSED

(both server and client) represents no connection state at all.

تنظیمات مربوط به vm

برای دیدن وضعیت هر کارت شبکه در برنامه های سیستم به دنبال virtual network editor میگردیم. در اینجا نشان میدهد که هر کارت شبکه به کدام یک از وضعیتهای nat , bridge , host only می باشد.

Host only به همه vm های داخلی را یک ای پی میدهد که این ای پی ها از بیرون دیده نمی شوند ولی شبکه بیرونی را میبینند . درواقع این ای پی ها در شبکه اصلی با ای پی اصلی دستگاهی که vm روی ان می باشد دیده میشوند.

Bridge یک ای پی مجزا گرفته می شود و از شبکه بیرونی نیز قابل رویت می باشد.

Host only فقط vm ها و کامپیوتر اصلی در یک شبکه دیده می شوند.

State : در این بخش وضعیت خط اتصال ( connection ) اعلام می شود. یک اتصال حالات مختلفی می تواند داشته باشد که آنها را معرفی می کنیم:

به معنای آنست که                                                                         وضعیت

هیچ اتصالی میان کامپیوتر شما و کامپیوتر راه دور وجود ندارد.                  CLOSED

کامپیوتر شما و کامپیوتر راه دور هر دو موافق خاتمه اتصال هستنند.         CLOSING

کامپیوتر راه دور اقدام به بستن اتصالش با شما کرده.                          CLOSE WAIT

اتصال پایداری برقرار شده است.                                                    ESTABLISHED

نرم افزاری که از این اتصال استفاده می کرده مانند یاهو مسنجر اکنون به

اتصال خود پایان داده                                                                     FIN WAIT1

کامپیوتر راه دور موافق بسته شدن اتصال است.                                  FIN WAIT2

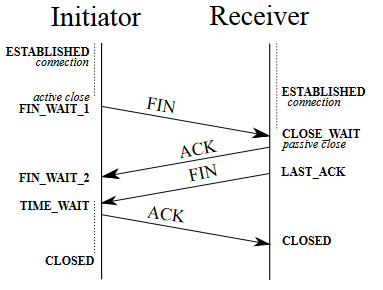
اتصال منتظر از بین رفتن تمامی بسته های اطلاعات است.                     LAST ACK

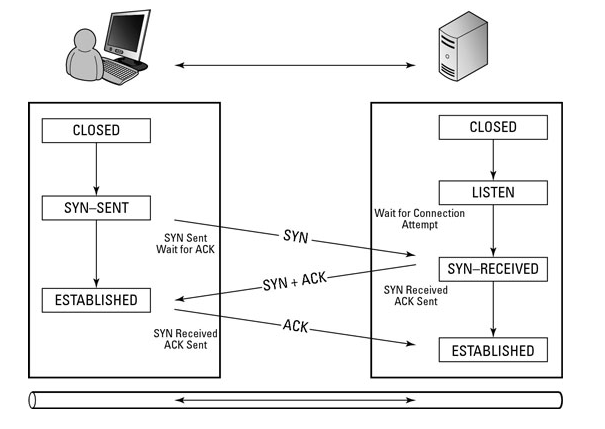
کامپیوتر شما در وضعیت شنود قرار گرفته تا پذیرای اتصال از خارج باشد.       LISTEN

کامپیوتر راه دور درخواستی را برای برقرار شدن اتصال می فرستد.            SYN RCVD

کامپیوتر شما برای باز شدن اتصالی اقدام کرده است.                             SYN SEND

همان کارایی LAST ACK را دارد.                                                      TIMED WAIT

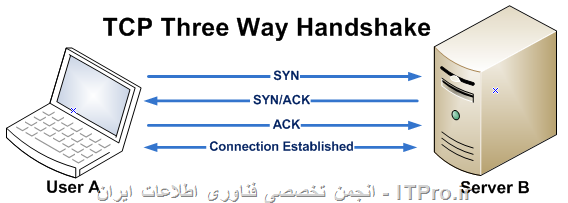




همانطور که قبلا هم در انجمن تخصصی فناوری اطلاعات ایران مطالعه کردید بصورت کلی ما پروتکل ها را از نظر نوع ارتبط به دو دسته اتصالگرا یا Connection Oriented و عدم اتصال گرا یا Connectionless تقسیم بندی می کنیم ، یکی از پروتکل های بسیار معروف در بحث اتصالگرا ، پروتکل TCP یا Transmission Control Protocol است که بیشترین استفاده را در ارتباطات مهم و حیاتی در سرویس ها بر عهده دارد. TCP برای برقراری ارتباط ابتدا باید درستی و صحت ارتباط تایید شود و سپس ارتباط برقرار شود ، فرآیند برقراری ارتباط در پروتکل TCP توسط یک فرآیند سه مرحله ای به نام Three-way Handshake یا Triple-Handshake انجام می شود ، در واقع هرگاه صحبت از Three-Way Handshake شد یعنی پروتکل ها قصد برقراری ارتباط با همدیگر را دارند ، فرآیند Three-Way Handshake در پروتکلی مثل TCP به شکل زیر انجام می شود :

1. ابتدا سیستم درخواست کننده یا مبدا که ما آن را Source خطاب می کنیم با آدرس IP فرضی 10.0.0.1 درخواست برقراری ارتباط خودش با آدرس مقصد یا Destination را بر روی پورت FTP به شکل 10.0.0.3:21 بر روی پورت نظر ارسال می کند که به این درخواست در اصطلاح SYN یا بسته اطلاعاتی SYN گفته می شود. SYN Packet مخفف Synchronization Packet است.
2. مقصد یا Destination بعد از اینکه درخواست را با استفاده از بسته اطلاعاتی SYN از مبدا دریافت کرد ، با استفاده از یک بسته اطلاعاتی به عنوان SYN//ACK به مبدا پاسخ می دهد که آماده برقراری ارتباط است . SYN//ACK مخفف کلمه های Synchronization Acknowledge است.
3. بسته اطلاعاتی ACK در نهایت از سمت مبدا یا Source به سمت مقصد ارسال می شود که نمایانگر دریافت کردن بسته SYN است

در نهایت بعد از اینکه Source یک بسته ACK در تایید برقراری ارتباط به Destination ارسال کرد ارتباط آماده برقراری است ، بعد از اینکه این فرآیند سه مرحله ای به درستی انجام شد به این معنی است که پورت FTP یا 21 ای که ما در اینجا درخواست داده ایم بر روی سرور باز یا Open است و آماده برقراری ارتباط است ، در حالت عادی بعد از برقرار شدن ارتباط Three Way Handshake فرآیند شروع ارتباط انجام می شود اما اگر اینکار توسط یک نرم افزار اسکنر انجام شود معمولا در نهایت در صورت بسته بودن پورت مورد نظر بسته اطلاعاتی FIN یا FINISH بعد از برقراری موفقیت آمیز ارتباط ارسال می شود و یا اینکه بسته RST یا Reset توسط نرم افزار ارسال می شود تا ارتباط بسته شود. همانطور که گفتیم این فرآیند در تمامی پروتکل های Connection oriented به این شکل انجام می شود.   
  
اگر بخواهیم مقایسه ای داشته باشیم برای درک بهتر این موضوع کافیست ساختار برقراری یک ارتباط تلفنی قدیمی را در نظر بگیریم ، شما گوشی را بر می دارید و شماره شخص مورد نظرتان را میگیرید ( همان پورت FTP ای که درخواست دادیم ) سپس بعد از برقراری ارتباط تلفنی و برداشتن گوشی تلفن شخص مورد نظر پاسخ می دهد الو بفرمایید ( شما میگید الو از بندست D: ) این کلمه الو همان SYN//ACK است و در نهایت شما می گویید سلام ، میخواستم در خصوص موضوعی با شما صحبت کنم و این همان فرآیند ACK آخر است که ارتباط ما آغاز می شود و صحبت های دو نفر از اینجا شروع می شود ، نکنید این کارارو بده زشته ... D:



FLAG های مختلف ارتباطی در TCP Connection

در ارتباطات استانداردی که در پروتکل TCP انجام می شود اولین قسمتی که برای برقراری ارتباط بررسی می شود در ساختار بسته اطلاعاتی قسمتی به نام TCP Packet Header و به ویژه قسمتی به نام FLAG است ، در واقع قسمت FLAG ابتدا بررسی می شود و بعد از بررسی های لازم ارتباط بین سیستم ها برقراری می شود و دستورات به سیستم ها داده می شود ، در این قسمت از بسته اطلاعاتی FLAG های مختلفی دیده می شوند که مهمترین آنها به شرح زیر می باشند :

1. SYN : این FLAG به معنی Synchronization است و اطلاع رسانی در خصوص ارسال یک Sequence Number جدید می باشد
2. ACK : این FLAG به معنی Acknowledge است و تاییده دریافت یک ارتباط و شناسایی Sequence Number بعدی می باشد
3. URG : این FLAG به معنی Urgent است و به معنی پردازش سریع داده های موجود در دستور در سریعترین زمان ممکن است
4. FIN : این FLAG به معنی FINISH با پایان است و اعلام می کند که دیگر قرار نیست بسته اطلاعاتی به سمت مقصد ارسال شود
5. RST : این FLAG به معنی RESET است و همانطور که از نامش هم پیداست برای RESET کردن ارتباط مورد استفاده قرار می گیرد

اسکن کردن با SYN یا SYN Scanning معمولا با استفاده از سه FLAG معروف SYN و ACK و RST انجام می شود.شما می توانید با استفاده از این FLAG ها و بعضا دستکاری کردن بسته های اطلاعاتی ارسالی به سمت سرور اطلاعات بسیار خوبی در خصوص پورت ها و سرویس های سیستم هدف بدست بیاورید که در فرآیند Enumeration بیشتر انجام می شود. تصویر محل قرارگیری Flag ها در پروتکل TCP را در بالا می توانید مشاهده کنید که در قسمت Header قرار گرفته است. ITPRO باشی

TCP states visited by ClientSide –  
https://cdncontribute.geeksforgeeks.org/wp-content/uploads/CN-1.png

TCP states visited by ServerSide –  
https://cdncontribute.geeksforgeeks.org/wp-content/uploads/CN-2.png