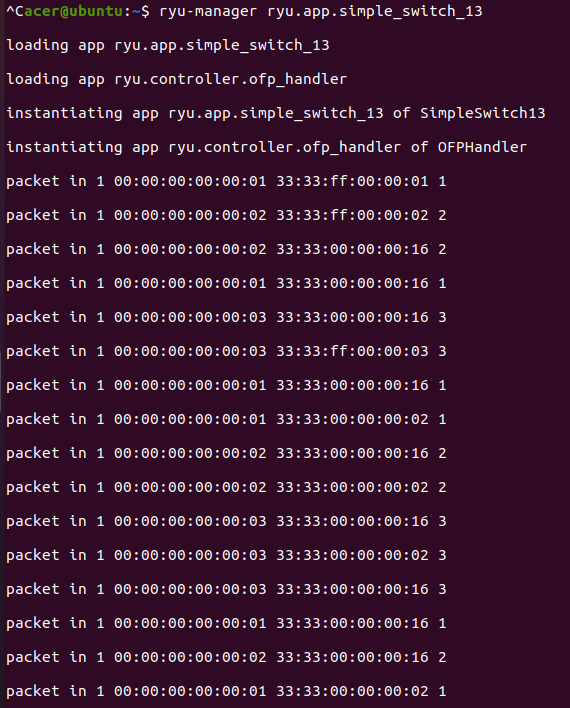
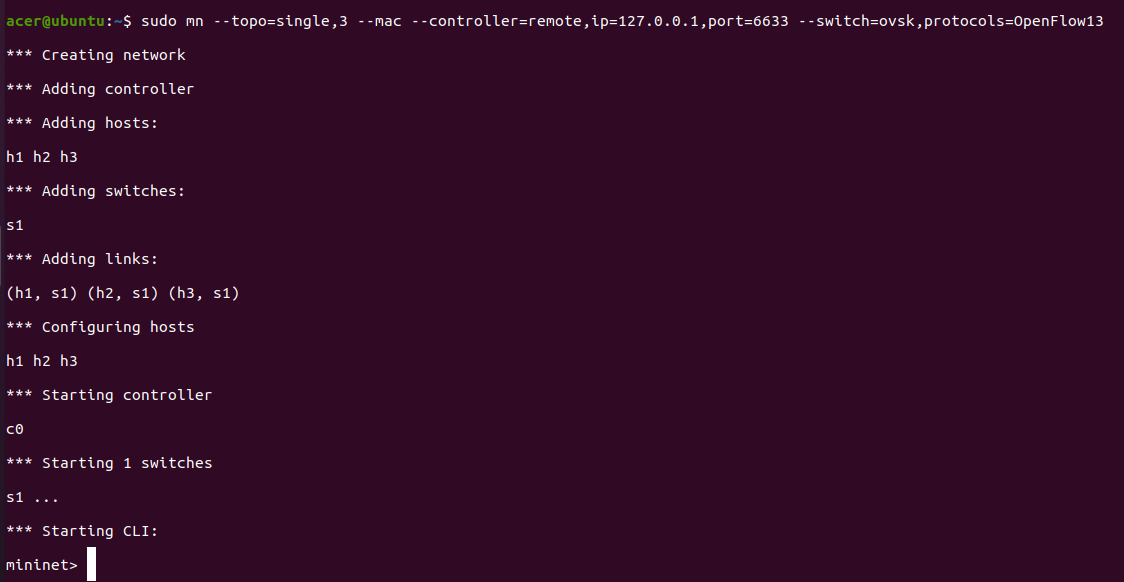
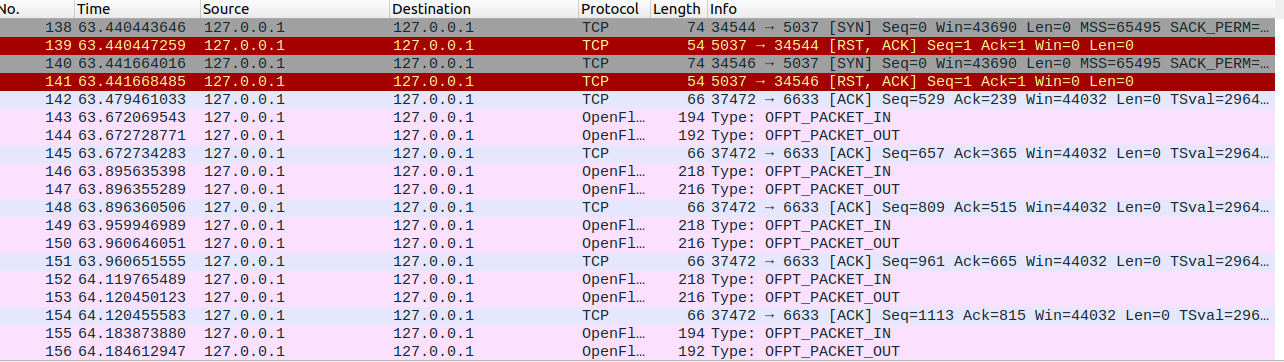
پروژه 2 شبکه 2\_ سارا سلطانی \_9823033

سوال 1: وایرشارک به مدیران شبکه این امکان را می‌دهد که ترافیک شبکه را به صورت بلادرنگ مانیتور کنند و به محض وقوع هر گونه مشکل یا تهدید، اقدامات لازم را انجام دهند. همچنین وایرشارک می‌تواند بسته‌های شبکه را ضبط کرده و آنها را تجزیه و تحلیل کند. این ابزار می‌تواند اطلاعات دقیقی از هر بسته شامل منبع، مقصد، پروتکل‌های استفاده شده و محتوای بسته‌ها را نمایش دهد. این اطلاعات می‌تواند به شناسایی مشکلات عملکردی مانند تنگناها، تاخیرها و از دست رفتن بسته‌ها کمک کند. علاوه بر آن وایرشارک می‌تواند الگوهای غیرعادی در ترافیک شبکه را شناسایی کرده و به مدیران شبکه هشدار دهد. وایرشارک می‌تواند به شناسایی مشکلات مرتبط با تنظیمات نادرست پروتکل‌ها، نسخه‌های ناسازگار، و خطاهای پروتکل کمک کند.

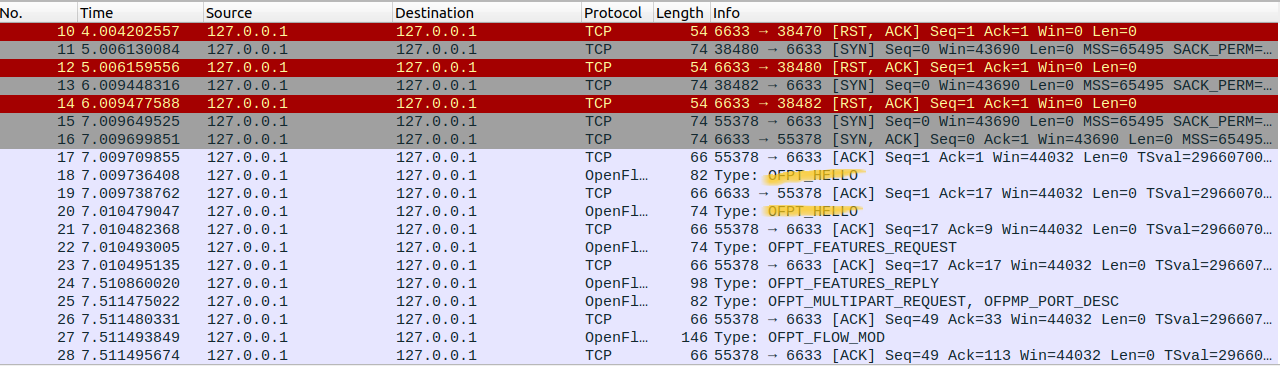
1\_2: پروتکل های open flow , tcp





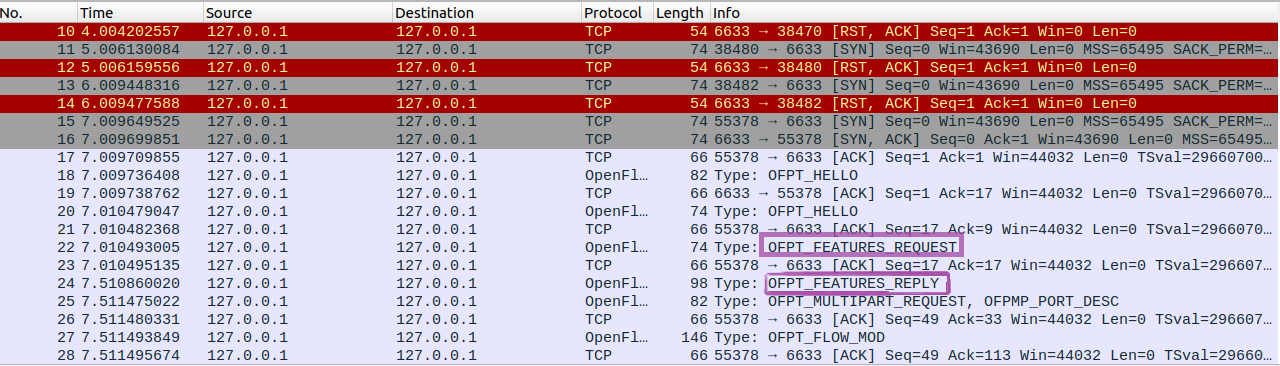


2\_2:

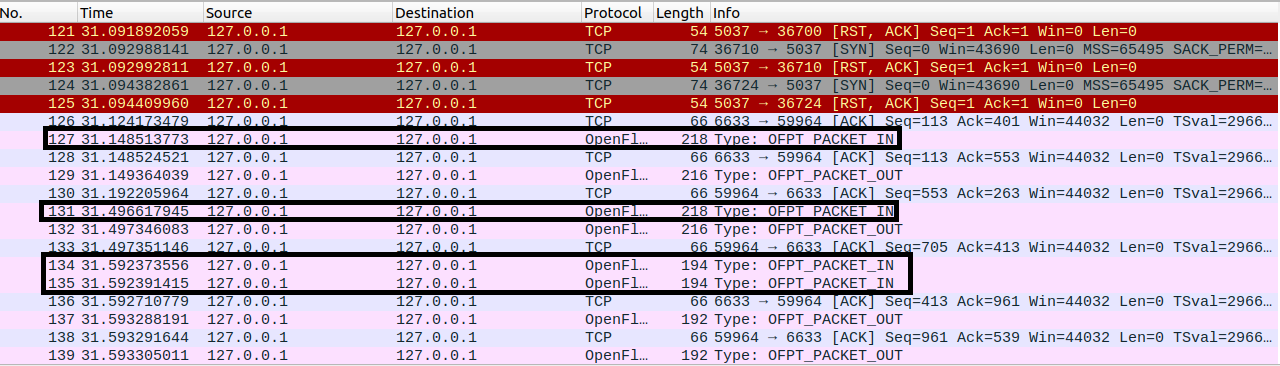


3\_2: در ابتدا کنترلر یک بسته به نام features\_request برای سوییچ میفرستد تا DPID و قابلیت ها و ویژگی های سوییچ را درخواست کند. این پیغام شامل هدر openflow است و بدنه آن خالی است. در پاسخ به کنترلر سوییچ یک پیغام features\_reply میفرستد که شامل تمامی اطلاعات درخواستی کنترلر یعنی DPID و ویژگی ها و قابلیت های سوییچ است. به طور کلی این پیغام ها رد و بدل شده تا کنترلر تمامی اطلاعات سوییچ را بدست آورده و براساس نیاز های شبکه آن را پیکر بندی کند.

DPID در واقع یک شناسه منحصر به فرد برای هر سوییچ است که کنترلر بوسیله این شناسه این سوییچ را در نظر گرفته و میشناسد.



4\_2:



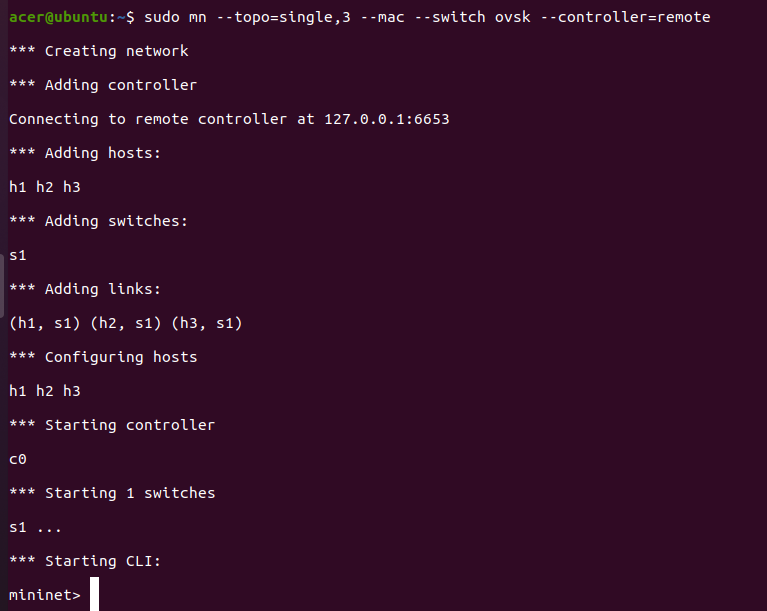
5\_2: یکی از این حالات table miss entry است و زمانی رخ میدهد که بسته به سوییچ می‌رسد و هیچ قانون تطابقی برای آن در جدول جریان (Flow Table) سوییچ وجود ندارد، سوییچ بسته را به کنترلر ارسال می‌کند که همان packet\_in است. این حالت به کنترلر اجازه می‌دهد تا در مورد چگونگی رسیدگی به بسته تصمیم‌گیری کند. این فرآیند به کنترلر امکان می‌دهد که قوانین جدید را ایجاد کرده و به سوییچ ارسال کند تا برای بسته‌های مشابه در آینده استفاده شوند. در واقع نیاز است کنترلر فلویی برای این بسته در نظر گرفته و در جدول انتری سوییچ قرار گیرد.

حالت دیگری که میتواند رخ دهد output to controller (action type) است. در برخی موارد، ممکن است قوانین جریان خاصی در جدول سوییچ وجود داشته باشد که مشخص میکند تا بسته‌های مچ شده با آن به کنترلر ارسال شوند. این دستورالعمل معمولاً برای بسته‌هایی استفاده می‌شود که نیاز به پردازش خاص توسط کنترلر دارند، مانند بسته‌های ARP، DHCP، یا هر نوع بسته‌ای که نیاز به تصمیم‌گیری پیچیده‌تر یا مدیریت مرکزی دارد. یا اگر نیاز به ایجاد یک قانون جدید در جدول مسیریابی برای آن بسته باشد این بسته به کنترلر ارسال میشود.

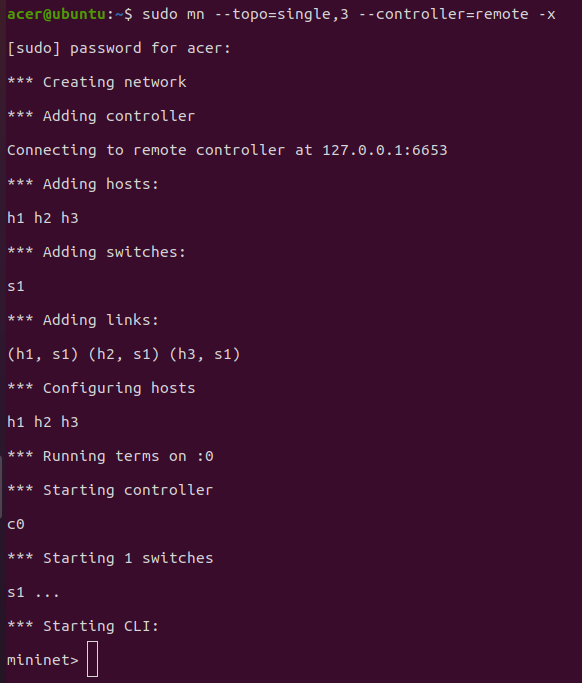
6\_2: از پروتکل openflow استفاده شده است. بسته های packet\_in نشان دهنده درخواست برای مک آدرس هاست دوم از طرف هاست اول هستند و در بسته های packet\_out پاسخ این درخواست ها قرار دارد که از طریق پاسخ هاست دوم به کنترلر به دست آمده است. در نتیجه این فرآیند مک آدرس هاست دوم به سوییچ و هاست اول انتقال داده میشود. در تمام این مراحل کنترلر به عنوان یک واسط تحت پروتکل openflow عمل میکند. در واقع وقتی سوییچ یک بسته پینگ دریافت میکند و نمیداند با آن چکار کند و چگونه برخورد کند سوییچ پیام های packet\_in ایجاد میکند.

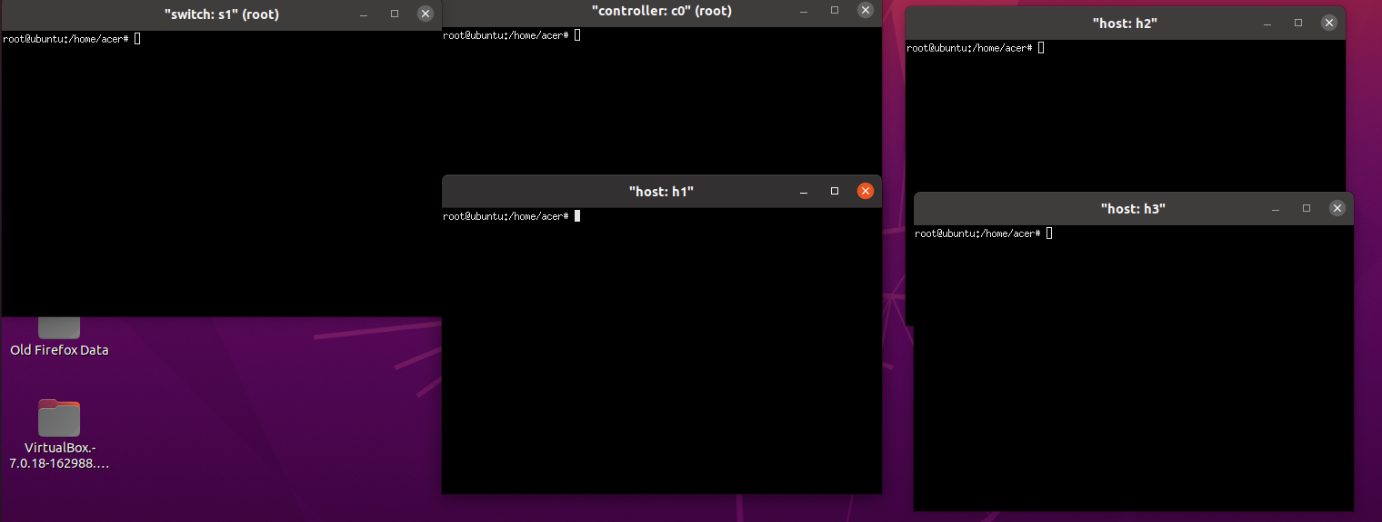


سوال 3: N=3 است.

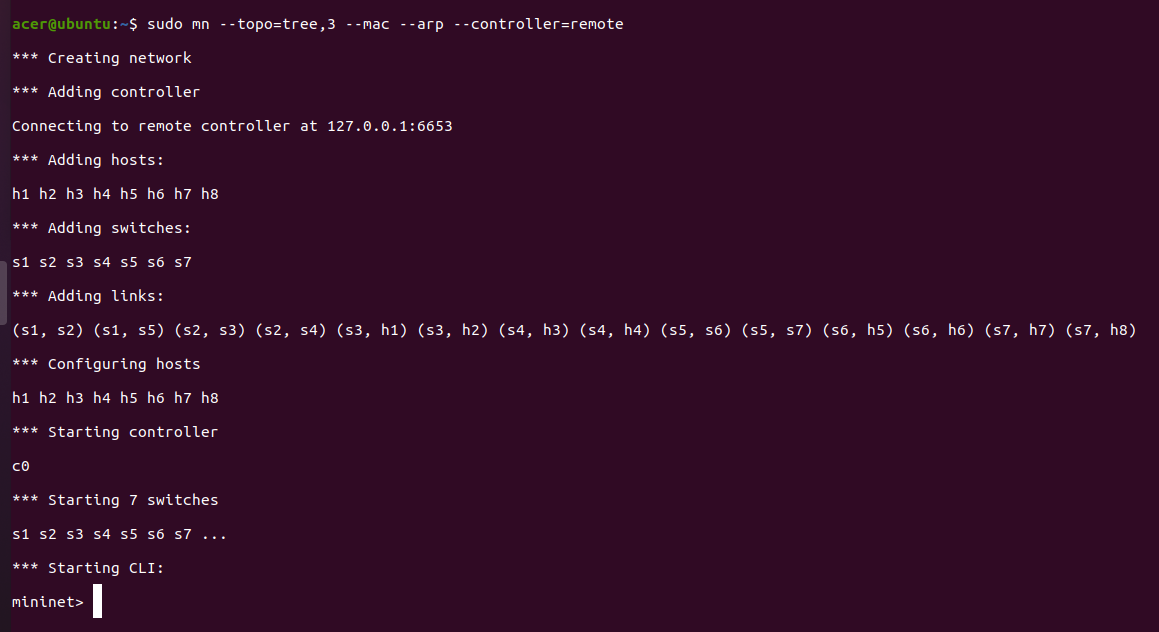


این دستور یک شبکه در mininet میسازد که شامل یک سوییچ و سه هاست متصل به آن است. از طرف دیگر –mac یک آدرس مک یکتا به هر هاست اختصاص میدهد و سپس آپشن –switch ovsk مشخص میکند که mininet از یک سوییچ open Vswitch که در سطح کرنل است استفاده میکند. و در آخر نیاز یک ریموت کنترلر برای کنترل مرکزی شبکه ساخته شده در نظر گرفته شده است.

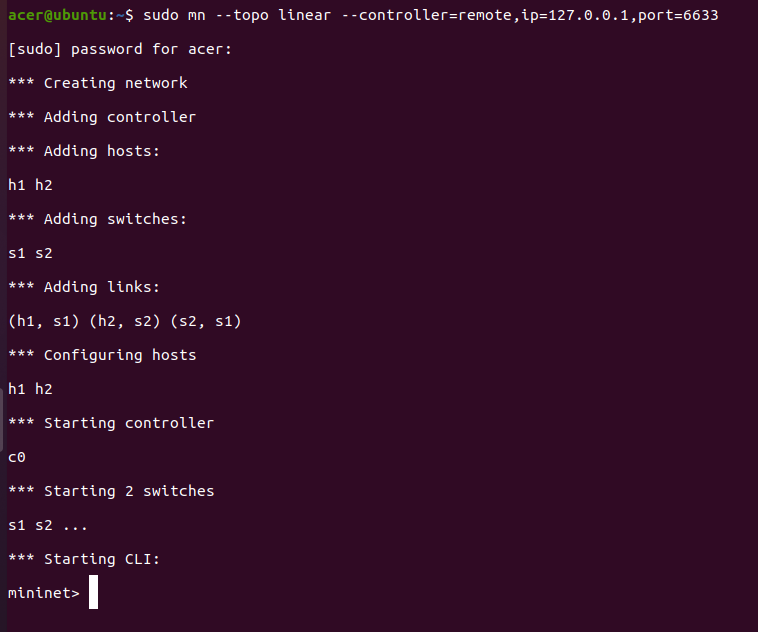




این دستور نیز مانند دستور قبلی یک شبکه سینگل با سه هاست در mininet ایجاد میکند. همچنین آپشن –controller remote نیز بک کنترلر ریموت مرکزی برای کنترل کل شبکه ایجاد کرده. آپشن -x نیز بک xterm برای هر هاست و سوییچ و کنترلر باز میکند تا بتوان با استفاده از آن به صورت اختصاصی تر پکت های دریافتی یا ارسالی برای هر کدام را مشاهده کرد.

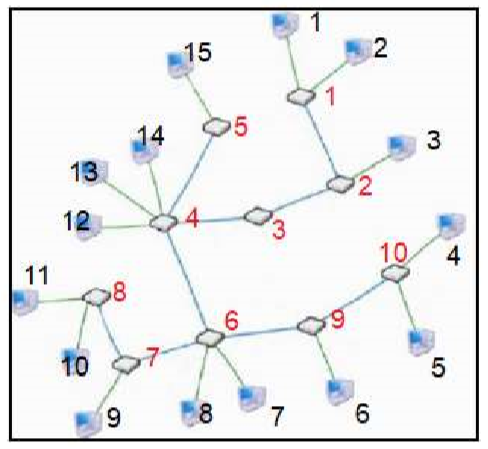
ای

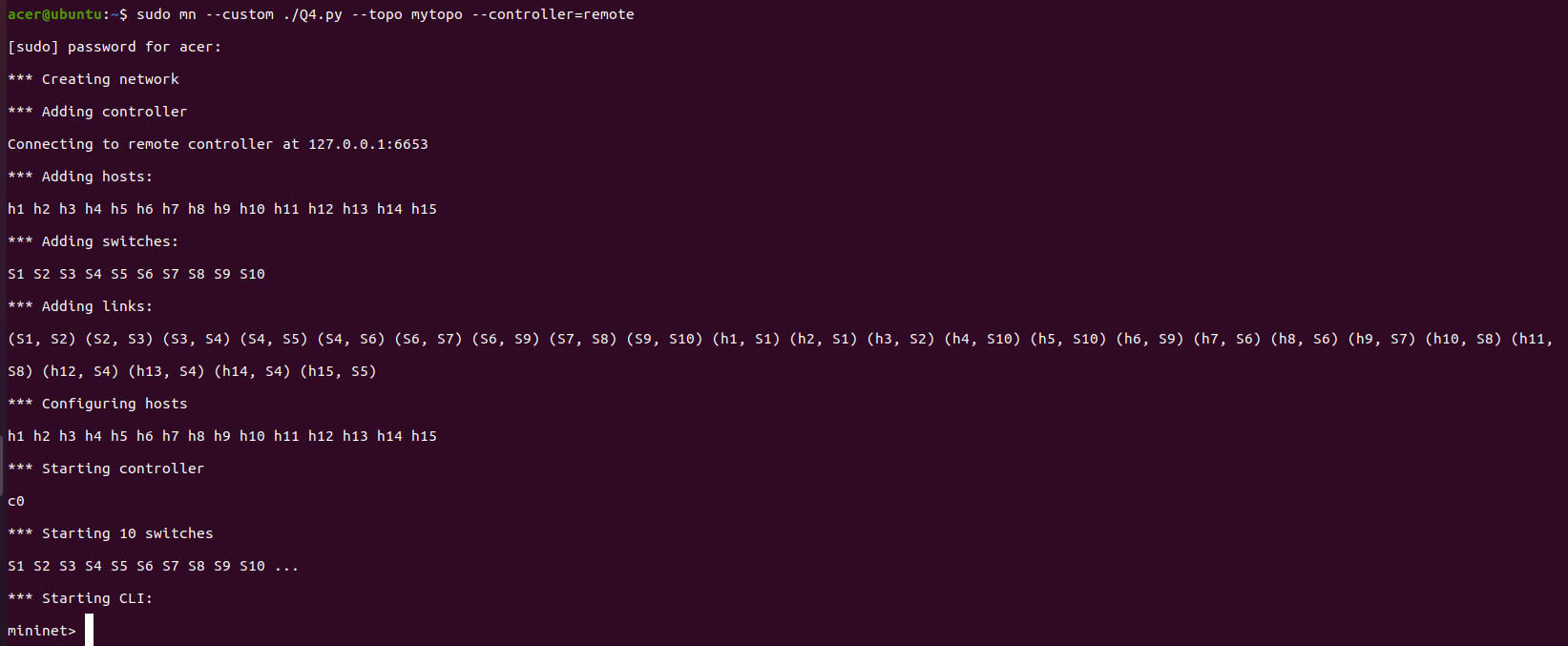
این دستور نیز یک شبکه درختی شامل 3 سطح ایجاد میکند که سوییچ ها به صورت سلسه مراتبی به هاست ها متصل بوده. آپشن –mac همانطور که قبا ذکر شد یک ادرس مک یکتا برای هر هاست در نظر گرفته. آپشن –arp نیز جدول arp هر هاست را با ورودی های یکدیگر پر میکند. مثلا اگر دو هاست h1 , h2 را داشته باشیم و از این آپشن استفاده کنیم به هاست h2 مک آدرسی که در جدول arp هاست h1 است را میدهد و برعکس.



این دستور یک شبکه با توپولوژی خطی ایجاد میکند که هر هاست آن به یک سوییچ مجزا متصل است. ابتدا یک کنترلر ریموت مانند قبل مشخص شده و سپس آیپی ادرس و شماره پورت کنترلر مورد نظر را به کنترلر اختصاص میدهد که در اینجا ما ادرس ایپی لوکال 127.0.0.1 و شماره پورت 6633را که مربوط به کنترلر ryu است در نظر گرفتیم.

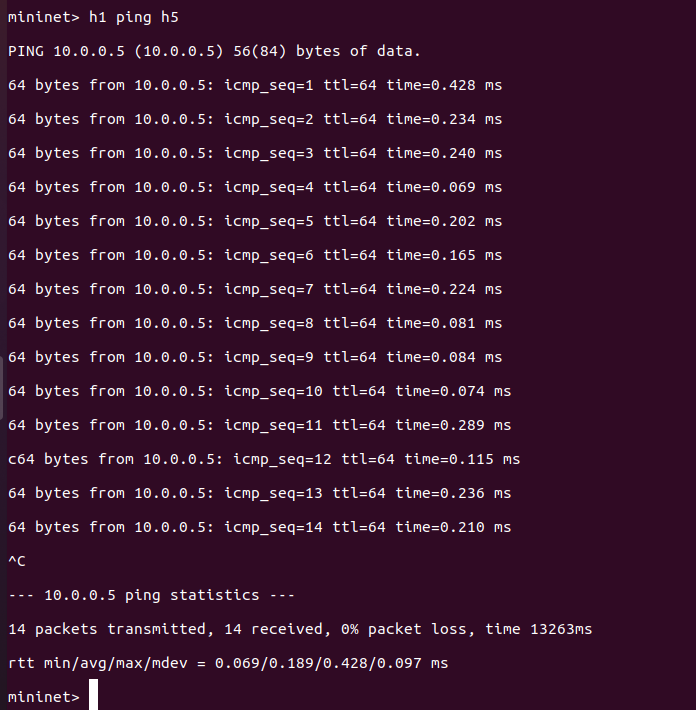
1\_4: کد پایتون براساس شماره گذاری های زیر نوشته شده است:

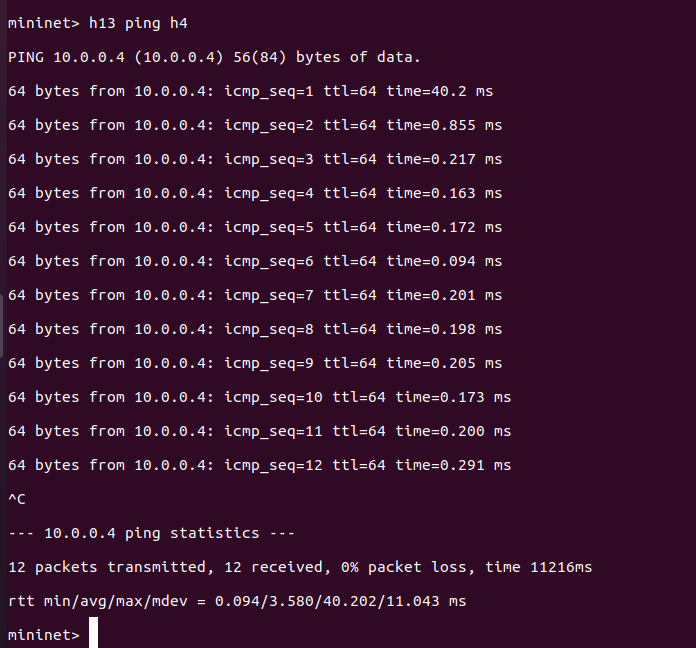


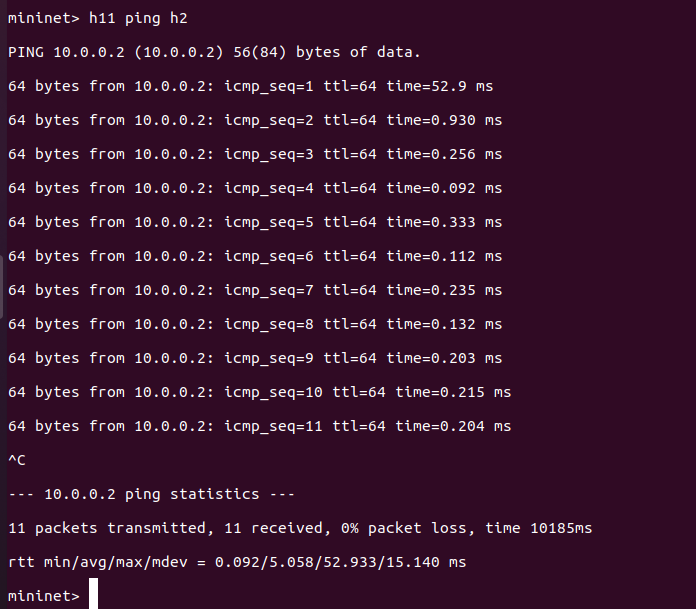


همانطور که در شکل نیز مشخص است 10 سوییچ و 15 هاست داریم.

2\_4:

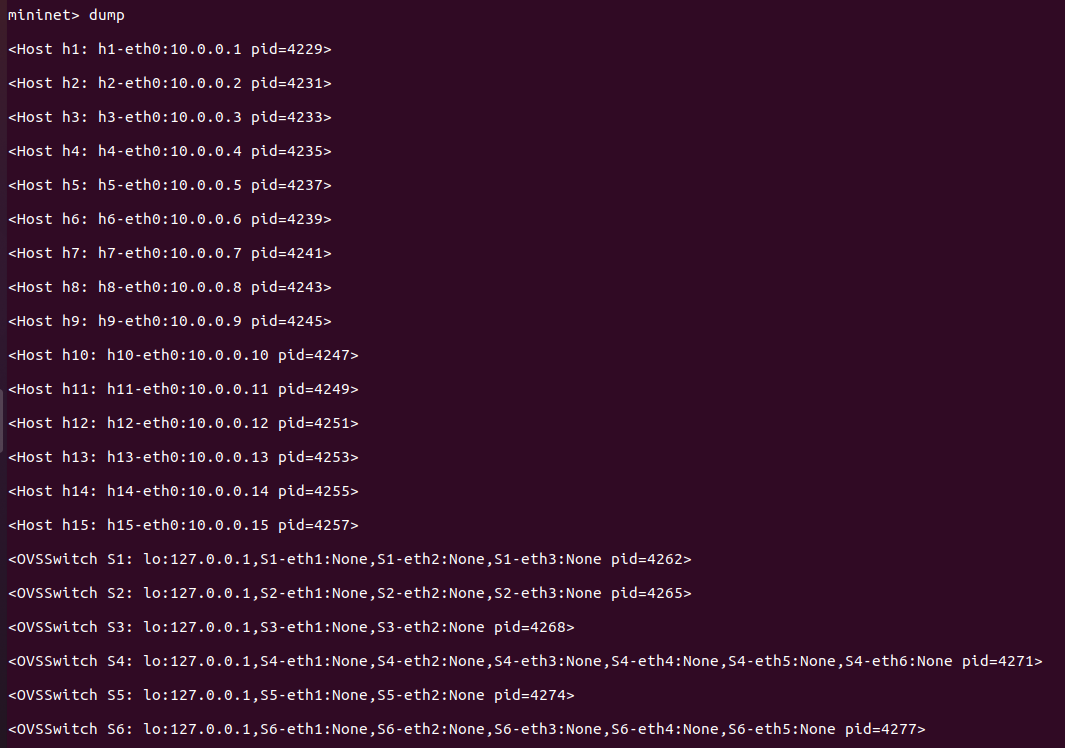


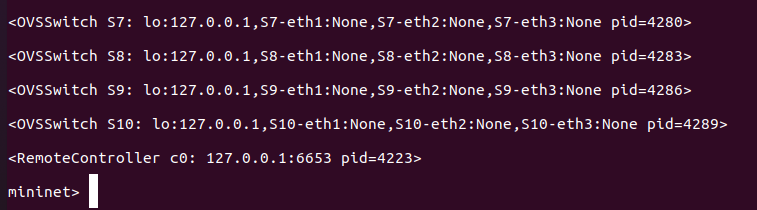




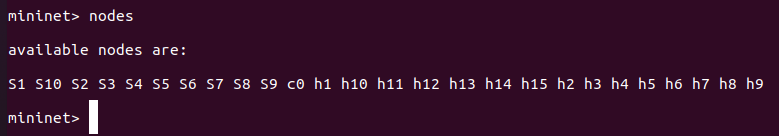
3\_4: به دلیل cold start latency زمان پینگ برای اولین تلاش بزرگتر از بقیه تلاش هاست. علت اصلی این مشکل این است که هنوز جداول arp اپدیت نشده اند. پس در اولین گام آپدیت کردن این جداول باید اتفاق بیفتد که خود کمی زمانبر است.

4\_4: نتیجه dump

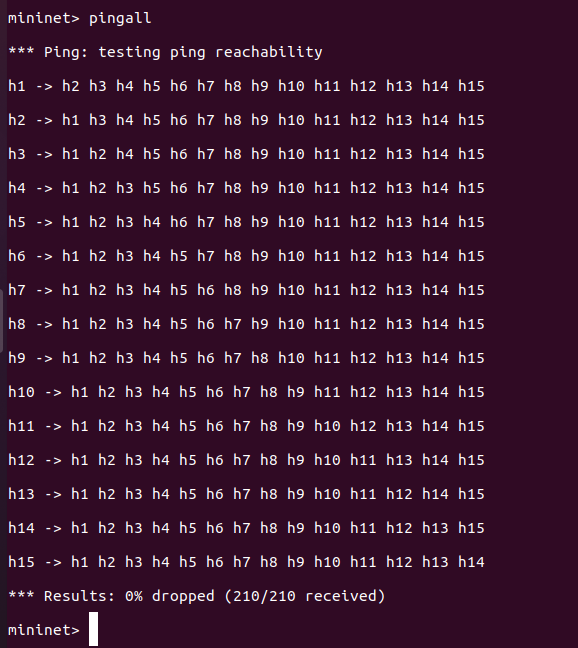




نتیجه nodes



نتیجه pingall



از تمامی هاست ها میتوان به یکدیگر بسته ارسال کرد و امکان پینگ وجود دارد.