۱- الف)

Destination Address	Interface
H3	3

ب)

Outgoing virtual circuit	Outgoing Interface	Incoming virtual circuit	Incoming Interface
22	3	12	1
18	4	63	2

۲- الف)

حداقل تعداد اسلات های زمانی مورد نیاز ۳ است. زمان بندی:

اسلات ۱: ارسال X در صف ورودی بالا، ارسال Y در صف ورودی میانی

اسلات ۲: ارسال X در صف ورودی وسط، ارسال Y در صف ورودی پایین

اسلات ۳: ارسال Z در صف ورودی پایین

ب)

بیشترین تعداد اسلات ها هنوز ۳ عدد است. در واقع، بر اساس این فرض که یک صف ورودی غیرخالی هرگز idle نیست، می بینیم که اولین اسلات زمانی همیشه شامل ارسال X در صف ورودی بالا و Y در صف ورودی وسط یا پایین می باشد. در اسلات زمانی دوم، همیشه می‌توانیم دو دیتاگرام دیگر ارسال کنیم و آخرین دیتاگرام را می‌توان در زمان سوم ارسال کرد. البته اگر اولین دیتاگرام در صف ورودی پایین X باشد، بدترین حالت به ۴ اسلات زمانی نیاز دارد.

۳- الف)

Prefix	Interface
11100000 00	0
11100000 01000000	1
1110000	2
11100001 1	3
otherwise	3

ب)

۱: پبشوند با حالت ۵ میخورد پس link ۳ میشود.

۲: پبشوند با حالت ۳ میخورد پس link ۲ میشود.

۳: پبشوند با حالت ۴ میخورد پس link ۳ میشود.

۴-

1) 2)Subnet A: 214.97.255/24 (256 addresses)
3)Subnet B: 214.97.254.0/25 - 214.97.254.0/29 (128-8 = 120 addresses)
4)Subnet C: 214.97.254.128/25 (128 addresses)

5)
Subnet D: 214.97.254.0/31 (2 addresses)
Subnet E: 214.97.254.2/31 (2 addresses)
Subnet F: 214.97.254.4/30 (4 addresses)

- **Forwarding table**

1 مسیریاب

Longest Prefix Match	**Outgoing Interface**
11010110 01100001 11111111	Subnet A
11010110 01100001 11111110 0000000	Subnet D
11010110 01100001 11111110 000001	Subnet F

2 مسیریاب

Longest Prefix Match	**Outgoing Interface**
11010110 01100001 11111111 0000000	Subnet D
11010110 01100001 11111110 0	Subnet B
11010110 01100001 11111110 0000001	Subnet E

3 مسیریاب

Longest Prefix Match	**Outgoing Interface**
11010110 01100001 11111111 000001	Subnet F
11010110 01100001 11111110 0000001	Subnet E
11010110 01100001 11111110 1	Subnet C

۵-

بله، بر اساس این مشاهدات، یک تکنیک ساده که می تواند برای شناسایی تعداد میزبان های منحصر به فرد در پشت NAT استفاده شود، تجزیه و تحلیل شماره شناسایی بسته های IP تولید شده توسط هر میزبان است. از آنجایی که اولین بسته تولید شده توسط یک میزبان دارای یک شماره شناسایی تصادفی است، می توانیم از آن به عنوان یک شناسه منحصر به فرد برای هر میزبان استفاده کنیم. با تجزیه و تحلیل شماره شناسایی تمام بسته های IP ارسال شده توسط NAT به دنیای خارج، می توانیم شماره های شناسایی منحصر به فرد را شناسایی کرده و تعداد میزبان های پشت NAT را بشماریم. همچنین از آنجایی که همه بسته‌های IP به خارج ارسال می‌شوند، بنابراین می‌توانیم از یک packet sniffer برای ضبط تمام بسته‌های IP تولید شده توسط میزبان‌های پشت NAT استفاده کنیم. از آنجایی که هر میزبان دنباله ای از بسته های IP با اعداد متوالی و یک شماره شناسایی اولیه مجزا (زیرا به طور تصادفی از یک فضای بزرگ انتخاب شده اند) تولید می کند (ID)، می توانیم بسته های IP را با شناسه های متوالی در یک خوشه گروه بندی کنیم. تعداد خوشه ها تعداد میزبان های پشت NAT است. با این حال، توجه به این نکته مهم است که این تکنیک فرض می‌کند که تمام بسته‌های IP تولید شده توسط میزبان‌های پشت NAT به دنیای خارج ارسال می‌شوند و هیچ دستگاه شبکه دیگری وجود ندارد که بتواند بسته‌هایی با شماره شناسایی تصادفی تولید کند. علاوه بر این، اگر NAT به گونه ای پیکربندی شده باشد که شماره شناسایی یکسانی را به همه بسته های تولید شده توسط یک میزبان اختصاص دهد، این تکنیک موثر نخواهد بود.

-۶

S2 Flow Table	
Match	**Action**
input Port = 3 / IP destination = 10.1.*.*	Forward (2)
input Port = 3 / IP destination = 10.3.*.*	Forward (2)
input Port = 4 / IP destination = 10.1.*.*	Forward (1)
input Port = 4 / IP destination = 10.3.*.*	Forward (1)