با سلام،

دستور کار چهارم درس آزمایشگاه شبکه با رویکرد آشنایی با پیاده سازی مکانیزم اختصاص IP با استفاده از پیکربندی پویای DHCP و همچنین آشنایی با پروتکل GRE خواهد بود.

پیاده‌سازی پروتکل پیکربندی پویای DHCP

با توجه به ساختار مدیریت دینامیک شبکه امروزه اختصاص آدرس های شبکه بصورت دینامیک صورت میپذیرد و پروتکل DHCP در شبکه به همین منظور ایجاد گردیده است. پروتکل پیکربندی پویا[1] (DHCP)، امکان تعریف IP برای مشتریان را به‌صورت پویا فراهم می‌آورد. هنگامی‌که تعداد کامپیوترها زیاد است، آدرس‌دهی و مدیریت آنها، بالطبع کار دشواری خواهد بود. از این‌روی، DHCP گزینه‌ی مناسبی در راستای برطرف نمودن این مشکل، محسوب می‌شود. تمام آدرس‌دهی‌ها و اعمال مرتبط در این راستا، در سرور DHCP، به‌صورت متمرکز، انجام می‌پذیرد.

از جمله مزایای DHCP می‌توان به ممانعت از تداخل IP و اعمال سلیقه‌های شخصی، و نیز سادگی و تمرکز در مدیریت پیکربندی میزبان اشاره نمود. شایان ذکر است، استفاده از DHCP مشکلاتی را با خود به‌همراه دارد. به‌عنوان مثال، سرویس‌گیرنده‌ها باید به هنگام فرایند راه‌اندازی، با سرور DHCP ارتباط برقرار کنند و تمامی اطلاعات مربوط به پیکربندی را دریافت نمایند. این امر موجب افزایش بار ترافیکی شبکه خواهد شد. همچنین، اگر در چنین شرایطی سرور DHCP قادر به پاسخگویی نباشد و یا تأخیر در پاسخگویی اتفاق بیفتد، مشکلات عدیده‌ای را با خود به‌همراه خواهد داشت.

پروتکل DHCP از دو بخش مهم تشکیل شده‌اند که عبارتند از: سرویس‌گیرنده[2] و سرویس‌دهنده[3]. منظور از سرویس‌گیرنده، سیستم و یا سیستم‌هایی است که به سرویس‌دهنده متصل می‌شوند و اطلاعات پیکربندی را به‌صورت خودکار از آن دریافت می‌کنند. تصویر زیر ارتباط میان این دو قسمت را نشان می‌دهد. همانگونه که در شکل مشخص است، سرویس‌گیرنده در ابتدا با ارسال پیام همه‌پخشی[4]، مبادرت به یافتن سرور می‌نماید. پس از آن، اطلاعات مربوط به پیکربندی، به سرویس‌گیرنده ارسال

---

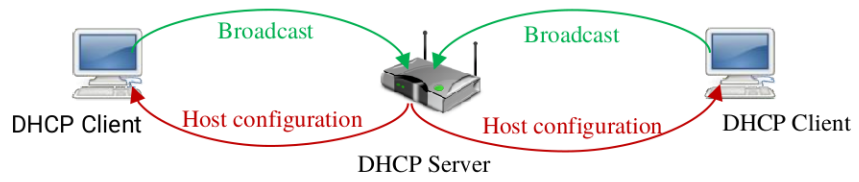
[1] Dynamic Host Configuration Protocol (DHCP)

[2] Client

[3] Server

[4] Broadcast

می‌شود. چناچه سرور در دسترس نباشد و یا تأخیر در پاسخ‌دهی اتفاق بیفتد، مشکلاتی را برای شبکه به‌همراه خواهد داشت:



شِمای کلی ارتباط میان سرویس‌دهنده و سرویس‌گیرنده در DHCP

سرویس‌گیرنده پیکربندی نمی‌شود و آدرس IP آن به 0.0.0.0 تنظیم خواهد شد.

- سرویس‌گیرنده به‌صورت خودکار و از طریق مکانیزم آدرس‌دهی IP خودکار انحصاری[5] (APIPA) یک آدرس به خود اختصاص خواهد داد. این آدرس تصادفی در محدوده‌ی 162.254.X.Y از کلاس B خواهد بود. مکانیزم APIPA دارای مشکلاتی است:
  - به‌جز IP و Mask، پارامتر دیگری را تنظیم نمی‌کند.
  - به‌صورت مداوم بررسی می‌کند که آیا آدرس تکراری است و یا خیر. از همین‌روی، ترافیک شبکه را افزایش می‌دهد.
  - غیر از 162.254.X.Y، نمی‌توان محدوده‌ی دیگری را روی آن تنظیم نمود.

  شایان ذکر است که در این روش، سرویس‌گیرنده پس از دریافت آدرس تصادفی، مجدداً بار یمدت کوتاهی (حدود ۵ دقیقه) به جستجوی DHCP می‌پردازد و اگر در این زمان موفق به یافتن آن نشد، از آدرس تصادفی موجود استفاده می‌کند.
- سرویس‌گیرنده، به‌صورت خودکار، با آدرس از پیش تعریف شده، تنظیم می‌شود.

نحوه‌ی عملکرد DHCP

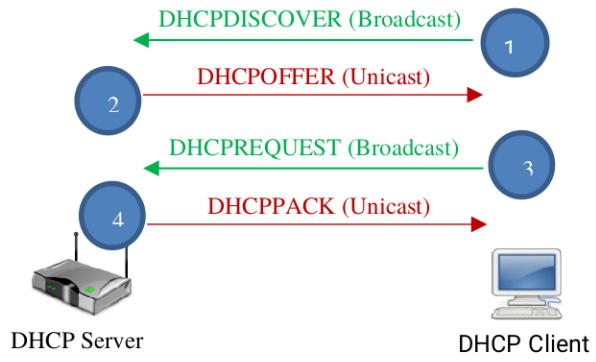
همانگونه که پیش از این مطرح گردید، DHCP جهت اعطای IP به‌صورت خودکار، به سرویس‌گیرندگان به‌کار می‌رود. پروتکل DHCP بر اساس مدل مشتری- خدمتگزار عمل می‌کند. در واقع، سرویس‌گیرندگان تقاضای خود را برای دریافت IP به سرور DHCP ارسال می‌کنند، و این سرور جزئیات پیکربندی را به آنها ارسال می‌نماید.

[5] Automatic Private IP Addressing (APIPA)

DHCP بر پایه ی پروتکل BOOTP عمل می‌کند. پروتکل BOOTP چارچوبی را برای عبور جزئیات پیکربندی در شبکه‌های TCP/IP، ارائه می‌دهد. از مزایای DHCP در BOOTP این است که نیازی نیست آدرس Mac تمام سرویس‌گیرندگان در سرور DHCP ثبت شود تا با استفاده از آن، IP دریافت کنند.

تصویر زیر، نحوه‌ی ارتباط میان مشتری و خدمتگزار را در DHCP نشان می‌دهد. همان‌گونه که در تصویر مشاهده می‌شود، ارتباط میان مشتری و خدمتگزار از چهار مرحله تشکیل شده‌است:

۱. سیستم عامل میزبان بر مبنای اخذ IP از سرور DHCP تنظیم می‌شود. بنابراین، سرویس‌گیرنده یک پیام DHCPServer به‌صورت همه‌پخشی ارسال می‌کند.
۲. سرور DHCP در همان شبکه‌ای قرار دارد که سرویس‌گیرنده نیز موجود است. این سرور، پارامترهای پیکربندی را پیشنهاد می‌دهد و پیام DHCPOFFER را به‌صورت تک‌پخشی[۶]، به سرویس‌گیرنده ارسال می‌کند.
۳. سرویس‌گیرنده، به این پیشنهاد DHCP پاسخ می‌دهد و پیام DHCPREQUEST را همه‌پخشی می‌کند.
۴. در نهایت، سرور DHCP آدرس IP را که به مشتری تخصیص یافته‌است، به‌صورت نهایی می‌پذیرد و پیام DHCPPACK را به‌صورت تک‌پخشی، به سرویس‌گیرنده ارسال می‌کند.



ارتباط میان سرویس‌دهنده و سرویس‌گیرنده در DHCP

تعادل بین سرویس‌گیرنده و سرور DHCP زمانی اتفاق می‌افتد که هر دو در یک محدوده از شبکه باشند. در غیر این‌صورت، علاوه بر این دو نیاز به رابطی است که در صورت درخواست IP توسط

---

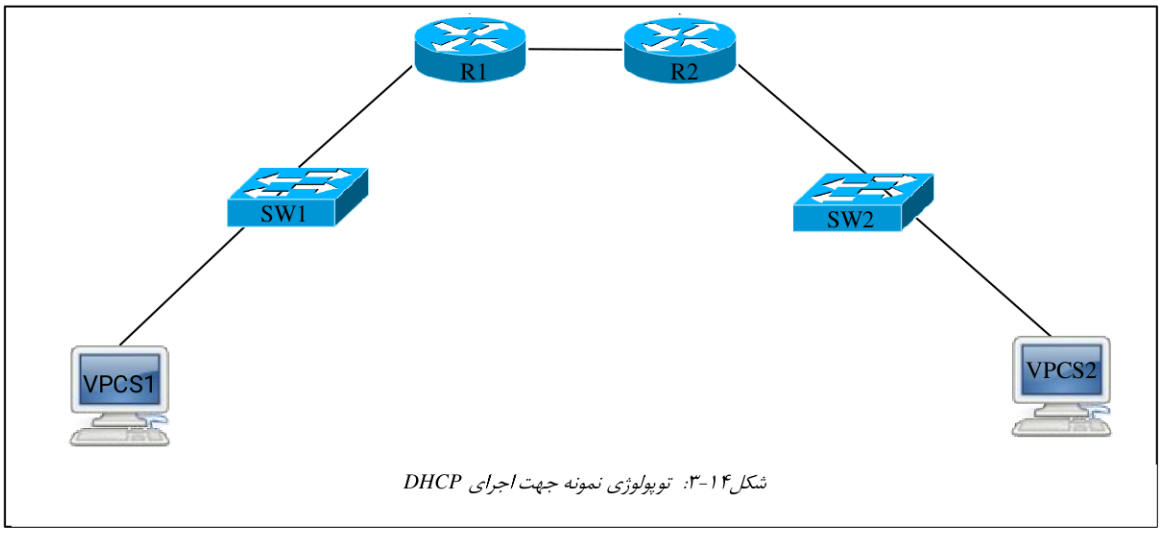
[۶] Unicast

مشتری، پیام‌ها را بین سرور و سرویس‌گیرنده رد و بدل نماید. به این رابط DHCP relay agent گفته می‌شود. یک relay agent می‌تواند یک مسیریاب باشد که پیام‌ها را از یک شبکه به شبکه‌ی دیگر انتقال می‌دهد.

آزمایش شماره ۱

✓ سناریو آزمایش اول

ابتدا نرم افزار GNS3 را از طریق سورس ارسال شده نصب و راه اندازی نمایید. سپس CISCO IOS 7200 را Mount کنید و از درستی نصب و راه اندازی روتر ۷۲۰۰ اطمینان حاصل نمایید. سپس توپولوژی زیر را در GNS3 بعنوان یک پروژه جدید و با نام شماره گروه خودتان ایجاد نمایید.



شکل۱۴-۳: توپولوژی نمونه جهت اجرای DHCP

انجام آزمایش DHCP

تصویر زیر توپولوژی مورد آزمایش را نشان می‌دهد. ابتدا ویدیو های بخش DHCP را مشاهده نمایید ا با مکانیزم ها آشنایی بیشتری پیدا نمایید. در این شکل، R_1 نقش سرور DHCP را ایفا می‌کند. در گام اول آزمایش، R_1 را تنظیم می‌کنیم تا به VPC1، آدرس IP اختصاص دهد. چون R_2 هنوز به عنوان Relayagent پیکربندی نشده‌است، VPCS2 آدرس IP دریافت نمی‌کند. در گام دوم آزمایش، R_2 را پیکربندی می‌کنیم تا VPCS2 نیز IP دریافت کند. بدین‌ترتیب، یک مخزن[7] IP به نام R_1 ایجاد می‌شود که شامل تمامی ipهای 192.168.1.0/24 است. آدرس 192.168.1.1 را به interface 0/0 مسیریاب

[7] IP Pool

R_1 دادیم تا سرویس‌گیرندگان از طریق آن، IP دریافت کنند. دستور *lease* نیز مدت زمانی را که IP به سرویس‌گیرنده تعلق می‌گیرد، نشان می‌دهد. دستور *excleded-address* هم از اختصاص IP متعلق به gateway، به سایر سرویس‌گیرندگان ممانعت به عمل می‌آورد. حال اگر VCPS1 را در حالت گرفتن IP به‌صورت اتوماتیک قرار دهیم، یک آدرس IP دریافت می‌کند. رای اینکه VPCS2 نیز از این سرور IP بگیرد، باید وارد R_2 شویم و در interface0/0 دستور *iphelper-address* را وارد نماییم. در قسمت بالا به جای کلمه‌ی IP باید آدرس IP مربوط به interface0/1 مسیریاب R_1 نوشته شود. حال اگر VPCS2 را نیز تنظیم کنیم، به‌صورت اتوماتیک IP دریافت می‌کند. برای انجام آزمایش سناریوی فوق را بطور کامل که شامل تمامی بخش های پیکربندی می شود بصورت ویدیویی نمایش دهید.

آزمایش شماره ۲

Wireshark Lab: DHCP v8.1

In this lab, we'll take a quick look at the Dynamic Host Configuration Protocol, DHCP. Recall that DHCP is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses to hosts, as well as to configure other network configuration information.

Before getting started, you'll probably want to review the coverage of DHCP in Section 4.4.3 in the text[8]. In particular, you'll want to pay close attention to Figure 4.24, since we'll be studying the DHCP Discover, Offer, Request and ACK messages shown in Figure 4.24.

As we've done in earlier Wireshark labs, you'll perform a few actions on your computer that will cause DHCP to spring into action, and then use Wireshark to collect and then the packet trace containing DHCP protocol messages.

Gathering a Packet Trace

The first two steps in the DHCP protocol in Figure 4.24 (using the Discover and Offer messages) are optional (in the sense that they need not always be used when, for example, a new IP address is needed, or an existing DHCP address is to be renewed); the Request and ACK messages are not. In order to

[8] References to figures and sections are for the 8th edition of our text, *Computer Networks, A Top-down Approach, 8th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.* Our website for this book is http://gaia.cs.umass.edu/kurose_ross You'll find lots of interesting open material there.

collect a trace that will contain all four DHCP message types, we'll need to take a few command line actions on a Mac, Linux or PC.

On a Mac:

2. In a terminal window/shell enter the following command:

```
% sudo ipconfig set en0 none
```

   Where `en0` (in this example) is the interface on which you want to capture packets using Wireshark. You can easily find the list of interface names in Wireshark by choosing Capture->options. This command will de-configure network interface `en0`.

3. Start up Wireshark, capturing packets on the interface you de-configured in Step 1.
4. In the terminal window/shell enter the following command:

```
% sudo ipconfig set en0 dhcp
```

   This will cause the DHCP protocol to request and receive an IP address and other information from the DHCP server.

4. After waiting for a few seconds, stop Wireshark capture.

On a Linux machine:

1. In a terminal window/shell, enter the following commands:

```
sudo ip addr flush en0
sudo dhclient -r
```

   where `en0` (in this example) is the interface on which you want to capture packets using Wireshark. You can easily find the list of interface names in Wireshark by choosing Capture -> Options. This command will remove the existing IP address of the interface, and release any existing DHCP address leases.
2. Start up Wireshark, capturing packets in the interface you de-configured in Step 1.
3. In the terminal window/shell, enter the following command:

```
sudo dhclient en0
```

   where, as with above, `en0` is the interface on which you are currently capturing packets. This will cause the DHCP protocol to request and receive an IP address and other information from the DHCP server.
4. After waiting for a few seconds, stop Wireshark capture.

On a PC:

1. In a command-line window enter the following command:

```
> ipconfig /release
```

   This command will cause your PC to give up its IP address.

2. Start up Wireshark.
3. In the command-line window enter the following command:

```
> ipconfig /renew
```

This will cause the DHCP protocol to request and receive an IP address and other information from a DHCP server.

4. After waiting for a few seconds, stop Wireshark capture.

After stopping Wireshark capture in step 4, you should take a peek in your Wireshark window to make sure you've actually captured the packets that we're looking for. If you enter "dhcp" into the display filter field (as shown in the light green field in the top left of Figure 1), your screen (on a Mac) should look similar to Figure 1.

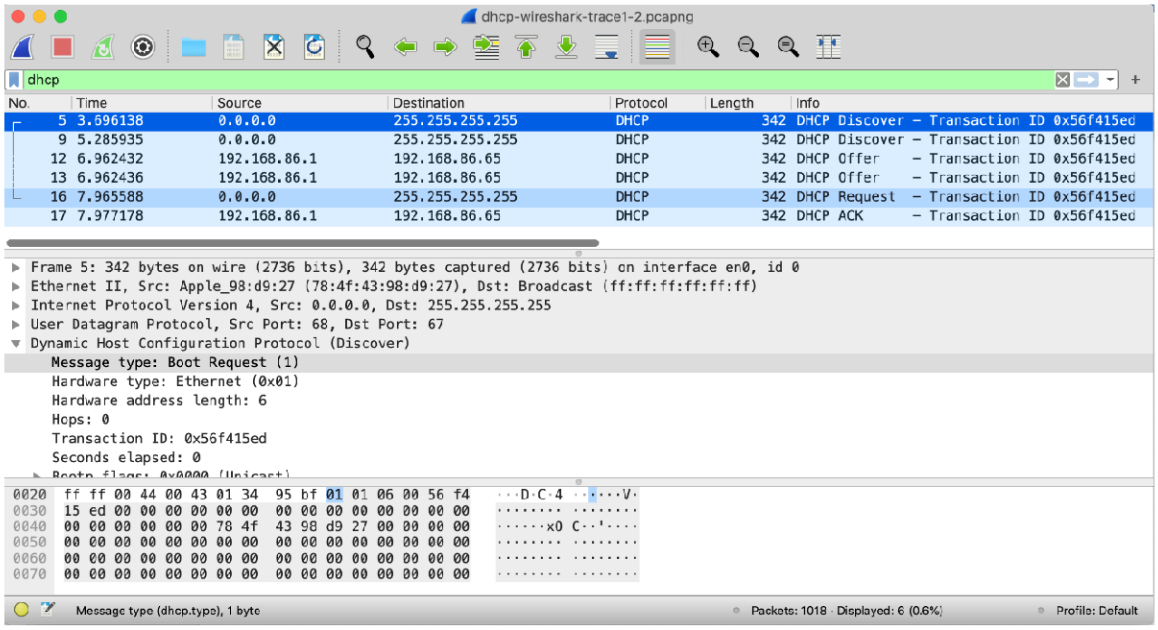


Figure 1: Wireshark display, showing the capture of DHCP Discover, Offer, Request and ACK messages

If you're unable to run Wireshark on a live network connection, are unable to capture all four DHCP messages, or are assigned to do so by your instructor, you can use the Wireshark trace file, *dhcp-wireshark-trace1-1.pcapng*[9] that we've gathered following the steps above on one of the author's

[9] You can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip and extract the trace file *dhcp-wireshark-trace1-1.pcapng.* These trace files can be used to answer these Wireshark lab questions without actually capturing packets on your own. Each trace was made using Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark

computers. You may well find it valuable to download this trace even if you've captured your own trace and use it, as well as your own trace, as you explore the questions below.

DHCP Questions

Answer the following questions[10]. If you're doing this lab as part of class, your teacher will provide details about how to hand in assignments, whether written or in an LMS.

Let's start by looking at the DHCP Discover message. Locate the IP datagram containing the first Discover message in your trace.

1. Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol?
2. What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain.
3. What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain.
4. What is the value in the transaction ID field of this DHCP Discover message?
5. Now inspect the options field in the DHCP Discover message. What are five pieces of information (beyond an IP address) that the client is suggesting or requesting to receive from the DHCP server as part of this DHCP transaction?

Now let's look at the DHCP Offer message. Locate the IP datagram containing the DHCP Offer message in your trace that was sent by a DHCP server in the response to the DHCP Discover message that you studied in questions 1-5 above.

6. How do you know that this Offer message is being sent in response to the DHCP Discover message you studied in questions 1-5 above?

lab. Once you've downloaded a trace file, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the trace file name.

[10] For the author's class, when answering the following questions with hand-in assignments, students sometimes need to print out specific packets (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the packet they've found the information that answers a question. They do this by marking paper copies with a pen or annotating electronic copies with text in a colored font. There are also learning management system (LMS) modules for teachers that allow students to answer these questions online and have answers auto-graded for these Wireshark labs at http://gaia.cs.umass.edu/kurose_ross/lms.htm

7. What is the *source* IP address used in the IP datagram containing the Offer message? Is there anything special about this address? Explain.
8. What is the *destination* IP address used in the datagram containing the Offer message? Is there anything special about this address? Explain. [Hint: Look at your trace carefully. The answer to this question may differ from what you see in Figure 4.24 in the textbook. If you really want to dig into this, consult the DHCP RFC, page 24.]
9. Now inspect the options field in the DHCP Offer message. What are five pieces of information that the DHCP server is providing to the DHCP client in the DHCP Offer message?

It would appear that once the DHCP Offer message is received, that the client may have all of the information it needs to proceed. However, the client may have received OFFERs from multiple DHCP servers and so a second phase is needed, with two more mandatory messages – the client-to-server DHCP Request message, and the server-to-client DHCP ACK message is needed. But at least the client knows there is at least one DHCP server out there! Let's take a look at the DHCP Request message, remembering that although we've already seen a Discover message in our trace, that is not always the case when a DHCP request message is sent.

Locate the IP datagram containing the first DHCP Request message in your trace, and answer the following questions.

10. What is the UDP source port number in the IP datagram containing the first DHCP Request message in your trace? What is the UDP destination port number being used?
11. What is the source IP address in the IP datagram containing this Request message? Is there anything special about this address? Explain.
12. What is the destination IP address used in the datagram containing this Request message. Is there anything special about this address? Explain.
13. What is the value in the transaction ID field of this DHCP Request message? Does it match the transaction IDs of the earlier Discover and Offer messages?
14. Now inspect the options field in the DHCP Discover message and take a close look at the "Parameter Request List". The DHCP RFC notes that

    > "The client can inform the server which configuration parameters the client is interested in by including the 'parameter request list' option. The data portion of this option explicitly lists the options requested by tag number."

    What differences do you see between the entries in the 'parameter request list' option in this Request message and the same list option in the earlier Discover message?

Locate the IP datagram containing the first DHCP ACK message in your trace, and answer the following questions.

15. What is the source IP address in the IP datagram containing this ACK message? Is there anything special about this address? Explain.
16. What is the destination IP address used in the datagram containing this ACK message. Is there anything special about this address? Explain.
17. What is the name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address?
18. For how long a time (the so-called "lease time") has the DHPC server assigned this IP address to the client?
19. What is the IP address (returned by the DHCP server to the DHCP client in this DHCP ACK message) of the first-hop router on the default path from the client to the rest of the Internet?

آزمایش شماره ۳

همان گونه که در ابتدای ترم دیدیم یک شبکه‌ی کامپیوتری، متشکل از دو یا چند کامپیوتر یا تجهیزات الکترونیکی است که به یکدیگر متصل شده‌اند و امکان به اشتراک‌گذاری منابع و اطلاعات را فراهم می‌آورند. به‌صورت کلی، دو نوع ساختار کلی شبکه به نام‌های اینترنت، اینترانت وجود دارند. البته، طبقه‌بندی‌های دیگری نیز در شبکه وجود دارند که ابعاد یک شبکه را نشان می‌دهند. برای مثال، شبکه‌ی LAN برای نمایش شبکه‌های کوچک در حد یک ساختمان، شبکه‌ی MAN برای شبکه‌هایی در سطح یک شهر، و شبکه‌ی WAN برای شبکه‌هایی با گستردگی زیاد، و همچنین شبکه‌های WLAN را می‌توان عنوان نمود. این شبکه‌ها و به‌ویژه شبکه‌هایی که از اینترنت استفاده می‌کنند، از پروتکل‌های ارتباطی مختلفی برای برقراری ارتباط بین کاربران در سطح شبکه استفاده می‌نمایند. یک بسته‌ی اطلاعاتی یا Packet، شامل اطلاعات کنترلی است که بررسی مواردی از قبیل اطمینان از رسیدن اطلاعات به مقصد، شناسایی خطاهای احتمالی و تصحیح آنها، و غیره را بر عهده دارد. یکی از این بسته‌های اطلاعاتی که بیشترین استفاده را در سطح اینترنت دارد، بسته‌های اطلاعاتی پروتکل (IP) است که در واقع، مهمترین پروتکل مورد استفاده در اینترنت است. این پروتکل، وظیفه‌ی مسیریابی کامپیوترها و دستگاه‌هایی را که از آدرس‌های IP برای برقراری ارتباط استفاده می‌کنند، بر عهده دارد. شبکه‌ها می‌توانند با استفاده از بسته‌های اطلاعاتی، فرایند آدرس‌دهی به چندین Host در شبکه و نیز خطایابی را به‌راحتی انجام دهند. حال، برای این‌که این اطلاعات در شبکه در حین انتقال در خطر شنود قرار نگیرد، لازم است ارتباطات IP با استفاده از پروتکل‌های رمزنگاری و احراز هویتی که ویژه‌ی IP Packetها و نشست[11] مربوط به آنها

[11] Session

هستند، رمزنگاری و احراز هویت شود. از جمله پروتکل‌های مورد استفاده برای این فرایندهای امنیتی که بیشترین استفاده را دارند، می‌توان پروتکل‌هایی نظیر Secure Socket Layer (SSL)، Secure Shell (SSH)، Transport Layer Security (TLS)، و Internet Protocol Security (IPsec) اشاره نمود.

پروتکل IPsec

IPsec، برای حفاظت از داده‌های اشتراکی بین دو Host، دو Gateway، و یا حتی یک Gateway و یک Host استفاده می‌شود. برخلاف سایر سیستم‌های امنیتی، حتی می‌توان از IPsec در نرم‌افزارهایی که برای استفاده از آن طراحی نشده‌اند نیز استفاده کرد. در زمانی‌که قرار است یک نشست ارتباطی ایجاد شود، پروتکل امنیتی IPsec به عامل‌ها[12] اجازه می‌دهد که یک احراز هویت دو طرفه[13] را انجام دهند و بر یک الگوریتم و کلید رمزنگاری برای رمزنگاری حین نشست ارتباط، توافق نمایند.

IPsec می‌تواند در هر دو حالت transport mode و tunnel mode، ارتباط طرفین را برقرار کند. IPsec، یک استاندارد جهانی است و می‌تواند با استفاده از مجموعه‌ای از پروتکل‌هایی که استفاده می‌کند، انواع و اقسام فرایندهای امنیتی را انجام دهد، از جمله پروتکل‌های مورد استفاده در IPsec، می‌توان به سرآیند (هِدر) احراز هویت (AH)[14] برای مقابله با حملات Replay، پروتکل کپسوله‌سازی پیلود امنیتی (ESP)[15] برای اعطای قابلیت محرمانگی به داده‌ها، و در نهایت، انجمن‌های امنیتی (SA)[16] برای ایجاد داده‌های مورد استفاده در AH و ESP، اشاره کرد.

کپسوله‌سازی مسیریابی عمومی (GRE)

پروتکل کپسوله‌سازی مسیریابی عمومی (GRE)[17]، یک پروتکل تونلینگ[18] است که برای انتقال سایر پروتکل‌های مسیریابی در یک شبکه‌ی مبتنی بر IP، مورد استفاده قرار می‌گیرد. تونلینگ، یک راه امن و اختصاصی برای انتقال بسته‌ها درمیان یک شبکه‌ی عمومی دیگر است. GRE، یک پروتکل کپسوله‌سازی IP است که برای انتقال بسته‌ها در طول یک شبکه استفاده می‌شود. اطلاعات، از طریق یک تونل GRE،

---

[12] Agents
[13] Mutual Authentication
[14] Authentication Header (AH)
[15] Encapsulating Security Payload (ESP)
[16] Security Associations (SA)
[17] Generic Routing Encapsulation (GRE)
[18] Tunneling

از یک شبکه به شبکه‌ای دیگر فرستاده می‌شود. GRE، یک پروتکل بدون حالت[19] است و هیچ‌گونه مکانیزمی برای جلوگیری از به‌وجود آمدن جریان[20] در ترافیک ندارد (فاقد مکانیزم کنترل جریان است).

GRE، بسته‌ها را درون بسته‌های IP کپسوله می‌کند و آنها را مجددا به‌سوی یک میزبان میانی، جایی‌که آنها به مقصد نهایی خود کپسوله و مسیریابی شده‌اند، هدایت می‌نماید. زیرا مسیریابی به میزبان میانی، برای دیتاگرام‌های داخلی به‌عنوان یک گام ظاهر می‌شود. سوییچ‌های اترنت سری، زمانی عمل می‌کنند که یک ارتباط نقطه به نقطه‌ی مجازی با یکدیگر دارند. تونل‌های GRE به پروتکل‌های مسیریابی اجازه می‌دهند همانند RIP و OSPF، بسته‌های داده را از یک سوییچ به سوییچ دیگر در طول اینترنت ارسال نمایند. علاوه بر این، تونل‌های GRE می‌توانند داده‌های چندپخشی را برای انتقال در طول اینترنت، کپسوله کنند.

سرآیند GRE

هدر GRE، شامل ۴ بایت است که حداقل سایز هدر GRE را بدون هیچ گزینه‌ی اضافی، نشان می‌دهد. اولین جفت از بایت‌ها (بیت ۰ تا ۱۵) شامل پرچم‌هایی است که حضور گزینه‌های GRE را نشان می‌دهد. اگر چنین گزینه‌هایی فعال باشند، سربار اضافی را به هدر GRE اضافه می‌کنند. دومین جفت از بایت‌ها، فیلد پروتکل است و نوع داده را که در تونل GRE حمل می‌شود، نشان می‌دهد. جدول زیر، گزینه‌های هدر GRE را توصیف می‌کند.

شماره بیت هدر	گزینه‌ها	توصیف
۰	نمایش checksum	اگر مقدار این بیت ۱ باشد، یک فیلد ۴ بایتی checksum را به هدر GRE، پس از فیلد پروتکل اضافه می‌کند.
۲	نمایش کلید	اگر مقدار این بیت ۱ باشد، یک کلید رمزنگاری ۴ بایتی را به هدر GRE، پس از فیلد checksum اضافه می‌کند.
۳	نمایش شماره‌ی ترتیبی	اگر این بیت ۱ باشد، یک شماره‌ی ترتیبی ۴ بایتی را به هدر GRE، پس از فیلد کلید اضافه می‌کند.
۱۳-۱۵	نسخه‌ی GRE	۰، GRE پایه را نشان می‌دهد؛ درحالی‌که ۱، برای PPTP استفاده می‌شود.

- گزینه‌ی نمایش Checksum (بیت ۰)، یک فیلد Checksum ۴ بایتی اختیاری به هدر GRE اضافه می‌کند. این Checksum، پس از فیلد پروتکل در هدر GRE نشان داده می‌شود. به‌طور

[19] Stateless

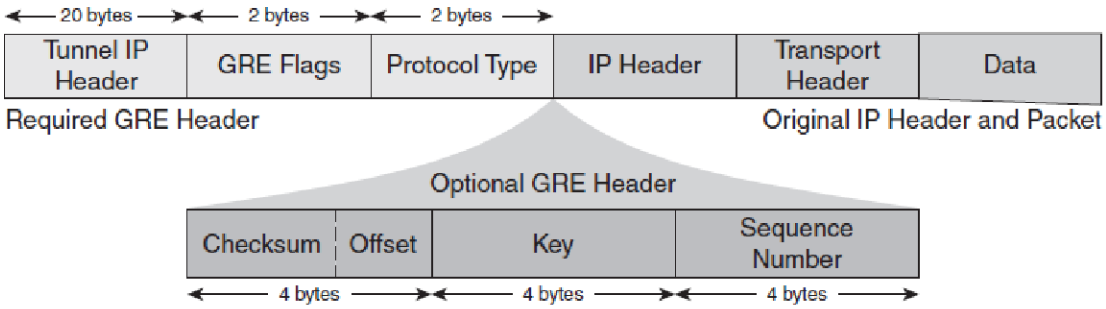
[20] Flow

طبیعی، به این گزینه نیازی نیست، زیرا سایر پروتکل‌های لایه‌های بالاتر، توانایی‌های Checksum را برای کشف خرابی بسته، فراهم می‌سازند.

- گزینه‌ی نمایش کلید (بیت ۲)، یک فیلد کلید ۴ بایتی اختیاری را به هدر GRE اضافه می‌کند. این کلید متنی آشکار، به دنبال فیلد checksum می‌آید تا زمانی‌که هر نقطه‌ی پایان GRE، کلید را در اختیار دارد، تصدیق نماید. با این‌وجود، خود کلید در هدر GRE، بدون محافظ است. به‌دلیل وجود این آسیب‌پذیری، معمولا پنهانی کردن GRE استفاده نمی‌شود. اما مقدار کلید می‌تواند استفاده گردد تا به‌طور یکتا، تونل‌های چندگانه را بین دو نقطه‌ی پایان، شناسایی نماید. این مورد می‌تواند شبیه یک IPsec SPI باشد.
- گزینه‌ی شماره‌ی ترتیبی (بیت ۳)، یک فیلد شماره‌ی ترتیبی ۴ بایتی اختیاری را به هدر GRE اضافه می‌کند. این مقدار ترتیبی، در ادامه‌ی گزینه‌ی کلید می‌آید و به این‌منظور استفاده می‌شود تا بسته‌های GRE را به‌محض ورود، به‌درستی و ترتیب، شناسایی نماید. همانند گزینه‌ی checksum، معمولا این مورد استفاده نمی‌شود، زیرا پروتکل‌های لایه‌ی بالاتر نیز این تابعیت را پیشنهاد می‌دهند.
- بیت ۱۵-۱۳، شماره‌ی نسخه‌ی GRE را نشان می‌دهد. ۰، GRE پایه و اولیه را نشان می‌دهد؛ درحالی‌که ۱، بیان می‌دارد که پروتکل تونلینگ نقطه به نقطه (PPTP)[21] در حال استفاده است. PPTP، در این مبحث توضیح داده نمی‌شود. دومین ۲ بایت از هدر GRE، فیلد پروتکل را نشان می‌دهد. این ۱۶ بیت، نوع بسته‌ای را در درون تونل GRE که در حال حمل است، شناسایی می‌کند. به‌عنوان مثال، نوع 0x0800، IP را نشان می‌دهد.

شکل زیر، یک بسته‌ی GRE را با تمام گزینه‌های اضافه‌شده به یک هدر IP و داده، نمایش می‌دهد. در این شکل، به‌طور معمول، تنها هدر GRE مورد نیاز، هدر IP اصلی، و بسته درپیکربندی تونل GRE ظاهر می‌شوند. معمولا گزینه‌های GRE استفاده نمی‌شوند، زیرا پروتکل‌های لایه‌ی بالاتر، تابعیت مشابه را فراهم می‌آورند.

[21] Point-to-Point Tunneling Protocol (PPTP)



فرمت بسته‌ی GRE

مقایسه‌ی GRE و IPsec

زمانی‌که IPsec محرمانگی داده‌ها را با استفاده از مکانیزم‌های احراز هویت تأمین می‌کند، پروتکل GRE از امنیت ضعیف‌تری برخوردار است و نمی‌تواند همانند IPsec امنیت ارتباط را تضمین نماید. همچنین، GRE دارای یک سرآیند بایت اضافی است که منجر به ایجاد تاخیر در فرآیند مسیریابی و ارسال بسته‌ها می‌گردد. اما با این‌وجود، IPsec فقط می‌تواند بسته‌ها را ارسال کند و فاقد قابلیت‌های GRE در ارسال پروتکل‌های مسیریابی است. در مقایسه‌ی خلاصه‌ی IPsec و GRE می‌توان موارد زیر را بیان نمود:

- IPsec، یکی از پروتکل‌های اصلی در اینترنت است در حالی‌که GRE، در این دسته قرار نمی‌گیرد.
- GRE می‌تواند سایر پروتکل‌های مسیریابی، مانند IP Packet را منتقل کند در حالی‌که IPsec قادر به انجام چنین کاری نیست.
- IPsec از درجه‌ی امنیتی بالاتری نسبت به GRE برخوردار است و این امر، ناشی از وجود مکانیزم‌های امنیتی این پروتکل است.
- GRE دارای یک هدر بایت است که باعث کند شدن فرایند مسیریابی و انتقال بسته‌ها می‌گردد، در حالی‌که در IPsec این‌گونه نیست.

مشخصه‌های GRE

قدرت اولیه‌ی GRE، قابلیت کپسوله شدن هر چیزی در آن بود. در ابتدا، از GRE جهت حمل بسته‌های غیر IP درون یک شبکه‌ی IP استفاده می‌گردید. همچنین، GRE به این‌منظور به‌کار گرفته می‌شد تا بسته‌های IP را درون یک ابر IP حمل کند. با استفاده از این روش، هدر اصلی IP، درون هدر GRE دفن می‌شود. ویژگی‌های عمومی یک تونل GRE عبارتند از:

- یک تونل GRE، شبیه یک تونل IPsec است، زیرا بسته‌ی اصلی، در یک پوسته‌ی بیرونی‌تر پیچیده می‌شود.

- GRE، پروتکلی بدون حالت است و هیچ مکانیزم کنترل جریانی را پیشنهاد نمی‌دهد.
- GRE، حداقل ۲۴ بایت از سربار، شامل ۲۰ بایت IP هدر جدید، را اضافه می‌کند.
- GRE، چندپروتکله است و می‌تواند هر پروتکل لایه‌ی سه مدل OSI را تونل‌سازی کند.
- GRE، به پروتکل‌های مسیریابی اجازه می‌دهد بین تونل رفت و آمد کنند.
- GRE، مورد نیاز بود تا ترافیک چندپخشی IP را به دوش بکشد. بعدها، نرم‌افزار IOS سیسکو 12.4(4)T را عرضه نمود.
- GRE از ویژگی‌های امنیتی نسبتا ضعیفی برخوردار است.

تونل GRE شبیه به یک تونل IPsec است. تونل، دو نقطه‌ی پایان دارد. ترافیک وارد یکی از پایان‌های تونل شده و از طرف دیگر خارج می‌شود؛ در حالی‌که درون تونل، مسیریاب‌ها از هدر بیرونی جدیدی تنها برای ارسال بسته‌ها استفاده می‌کنند. تونل GRE بدون حالت است. برخلاف یک تونل IPsec، نقطه‌های پایان، هیچ پارامتری را قبل از ارسال ترافیک میان تونل، هماهنگ نمی‌کنند. تا زمانی‌که مقصد تونل قابل مسیریابی است، ترافیک می‌تواند درون آن جریان پیدا کند. همچنین، GRE به‌صورت پیش‌فرض، هیچ ترتیب و قابلیت اطمینانی را فراهم نمی‌سازد. این ویژگی، به‌طور معمول، به‌وسیله‌ی پروتکل‌های لایه‌ی بالاتر مدیریت می‌شوند.

تونل‌های GRE، امنیت حداقلی دارند درحالی‌که IPsec، امنیت را توسط ابزارهای رمزدار و محرمانه، تصدیق داده‌ها، و ضمانت کامل ارائه می‌کنند. GRE، یک مکانیزم رمزگذاری اولیه دارد، اما کلید، در طول تونل، همراه بسته حمل می‌شود که تا حدی هدف را مغلوب می‌نماید. GRE، دارای ۲۴ بایت هدر اضافی و سرابار هست. این سربار، شامل ۲۰ بایت هدر IP جدید است که آدرس IP مبدا و مقصد تونل GRE را نمایش می‌دهد. ۴ بایت باقیمانده، هدر GRE است. گزینه‌های اضافی GRE می‌توانند هدر GRE را به بالای ۱۲ بایت دیگر افزایش دهند. شایان ذکر است، اندازه‌ی بسته‌ی بزرگتر، که بر اثر هدرهای اضافی به‌وجود آمده‌است، می‌تواند تاثیر مخربی روی کارآیی شبکه بگذارد زیرا هر بسته ای که در شبکه مسیریابی میشود عملا از نظر طول بسته دارای سربار اضافه خواهد بود و آدرس های مسیر یابی نیز در روتر ها پردازش مجدد می شوند. به‌دلیل این‌که هدرهای اضافی به‌طور پویا اضافه می‌گردند، بیشتر کاربران معتقدند در نتیجه، هیچ اتفاق بدی نمی‌تواند رخ دهد. اگر یک بسته، بزرگتر از واحد انتقال ماکزیمم (MTU)[۲۲] باشد، مسیریاب‌ها باید بسته را به قطعات کوچکتر تقسیم کنند تا متناسب باشد.

[22] Maximum Transmission Unit (MTU)

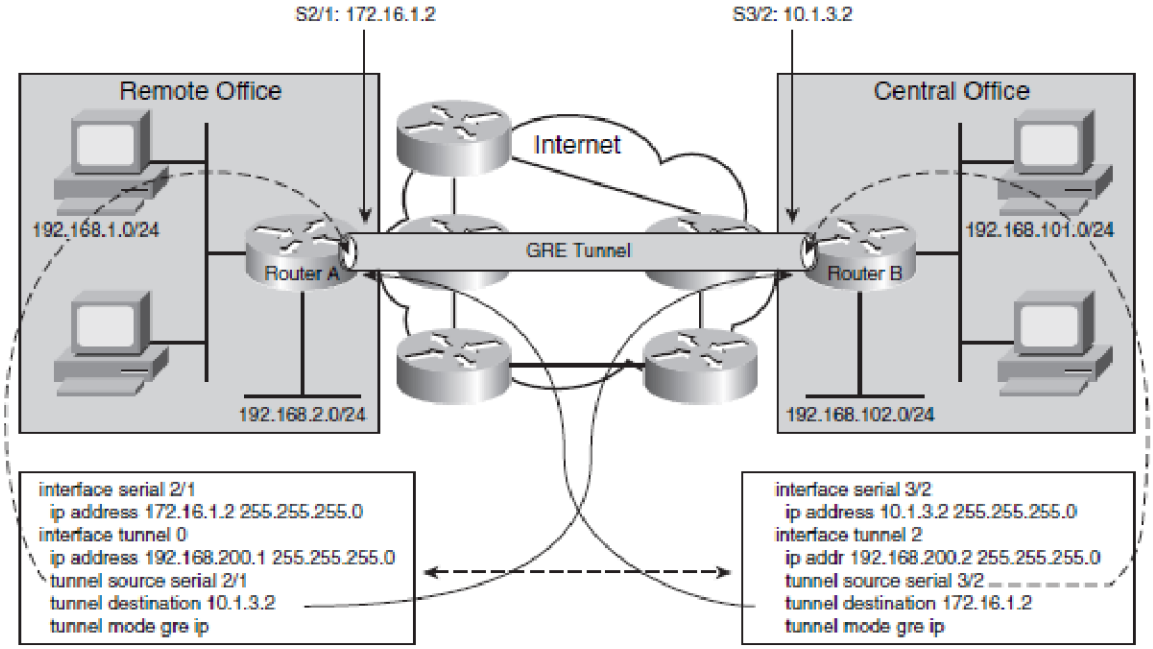
این تلاش برای تکه‌تکه کردن می‌تواند کار اضافی CPU را برای مسیریاب افزایش دهد. این مورد می‌تواند کل ارسال بسته را تحت تاثیر قرار دهد.

GRE، هنوز یک ابزار تونلینگ قدرتمند و ساده است و می‌تواند هر پروتکل لایه‌ی سه OSI را تونل‌سازی کند. به‌طور اساسی، یک ارتباط اختصاصی نقطه به نقطه، دو طرفه است. یک ارتباط خصوصی بین دو نقطه‌ی پایان، یک تعریف پایه از VPN است. برخلاف IPsec، GRE به پروتکل‌های مسیریابی (مانند OSPF و EIGRP) اجازه می‌دهد از خط ارتباط عبور کنند. تونل‌های IPsec می‌توانند بسته‌های IP را ارسال کنند، اما قادر به ارسال پروتکل‌های مسیریابی نیستند.

پیش از آن‌که بسته‌های IP بتوانند از طریق تونل IPsec عبور کنند، وجود مسیریاب‌های ایستا در هر نقطه‌ی پایان IPsec، برای اطلاع از مسیریابی انتهای مقابل، لازم است. این پیکربندی اضافی، با تعداد زیاد تونل‌های IPsec متناسب نبود. با عرضه‌ی نرم‌افزار IOS سیسکو 12.4(4)T، این مشکل برطرف گردید. IP چندپخشی باید روی GRE فرستاده شود. پیش از ارائه‌ی IOS، IPsec نمی‌توانست ترافیک چندپخشی IP را حمل کند. GRE به تنهایی دارای هیچ ویژگی امنیتی قوی نیست. هدر، یک مکانیزم کلید امنیت اختیاری و در عین حال ضعیف را فراهم می‌کند. در نتیجه، هیچ امنیت قوی، تصدیق منبع داده، یا مکانیزم درستی داده در GRE وجود ندارد. این در حالی است که IPsec، امنیت، تصدیق منبع، و درستی داده را با استفاده از MD5 یا SHA-1 HMACs فراهم می‌آورد. بنابراین، یک تونل GRE که ترافیک چندپخشی را حمل می‌کند، می‌تواند از طریق یک تونل IPsec، برای بالابردن امنیت فرستاده شود. طبیعتا استفاده از الگوریتم های رمزنگاری قدیمی و ناامن می تواند آسیب جدی در پیکربندی روتر بر مبنای IPSec باشد که در طراحی پروتکل امنیتی لایه سه شبکه باید به آن دقت کافی داشت.

پیکربندی اولیه‌ی GRE

یک تونل GRE، برخی از پروتکل‌های لایه‌ی ۳ را بین دو نقطه‌ی پایان IP حمل می‌کند. در طول استفاده‌ی اولیه از تونل GRE، معمولا محتوای تونل، هر پروتکلی به جز IP بود. امروزه، تونل‌های GRE استفاده می‌شوند تا داده‌ی IP را روی یک شبکه‌ی IP، حمل نمایند. اما خود تونل GRE می‌تواند جهت افزایش امنیت، از طریق یک تونل IPsec فرستاده شود. شکل زیر، یک تونل GRE اولیه را نشان می‌دهد.



تونل اولیه‌ی GRE

اجزای پیکربندی اولیه‌ی تونل GRE عبارتند از:

- یک مبدا تونل (یک آدرس IP محلی به این مسیریاب)
- یک مقصد تونل (یک آدرس IP از یک مسیریاب دور)
- یک مد تونل (GRE/IP پیش‌فرض است)
- ترافیک تونل (داده‌ای که از طریق تونل، جابه‌جا و به‌وسیله‌ی هدر GRE، کپسوله می‌شود)

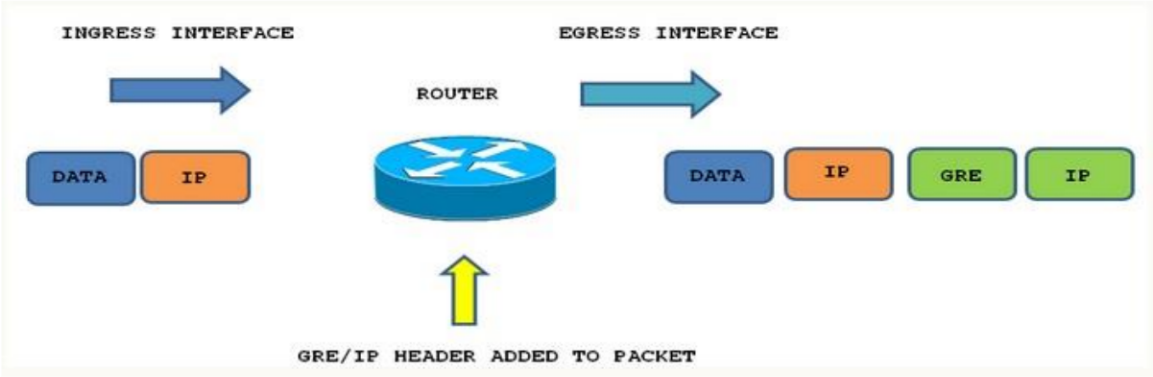
در شکل بالا، یک تونل GRE بین دو نقطه‌ی پایان IP وجود دارد که پیکربندی شده‌است. در واقع، تونل GRE به‌عنوان یک interface در هر مسیریاب تعریف شده‌است. Interface متعلق به GRE باعث می‌شود GRE، چندپروتکله باشد. یک واسط مسیریاب می‌تواند برای انتقال هر پروتکلی، پیکربندی گردد. پروتکل‌های در دسترس، به ویژگی‌های IOS سیسکو که تنظیم و نصب شده‌اند، وابسته هستند.

مبدا و مقصد تونل، interfaceهای IP هستند. بنابراین، GRE در طول یک شبکه‌ی IP عبور می‌کند. پروتکلی که در interfaceهای GRE پیکربندی شده، داده‌ای است که از طریق تونل GRE عبور می‌کند.

مبدا تونل GRE در یک سر باید با مقصد در سر دیگر، متناظر و معکوس باشد. این معتبرسازی IP زمانی اجرا می‌شود که تونل GRE برپا می‌گردد. برای مسیریابی درست از طریق GRE باید یک زیرشبکه‌ی مشترک در تونل پیکربندی شود. در شکل بالا، IP داخل تونل GRE پیکربندی شده‌است. تونل، در دو محل، از آدرس خصوصی RFC 1918 استفاده می‌کند. مسیریابی IP بین این دو محل، توسط ابزارهای پروتکل مسیریابی مورد علاقه‌ی کاربر، از طریق تونل GRE جریان می‌یابد. همچنین، برای مستندسازی اهداف شبکه‌ی عمومی، از آدرس خصوصی استفاده می‌کند؛ اگرچه، الزامی نیست.

نحوه‌ی پیکربندی تونل GRE

تونل‌سازی، یک مکانیزم انتقال بسته‌ها را از یک پروتکل درون پروتکلی دیگر فراهم می‌کند. پروتکلی که حمل می‌گردد، پروتکل مسافر نامیده می‌شود. همچنین، پروتکلی که برای حمل مسافر استفاده می‌گردد، پروتکل انتقال نامیده می‌شود. GRE، یکی از مکانیزم‌های تونل‌سازی در دسترس است که از IP به‌عنوان پروتکل انتقال استفاده می‌کند و می تواند برای حمل بسیاری از پروتکل‌های مسافر مختلف، استفاده گردد. تونل‌ها، به‌عنوان لینک‌های نقطه به نقطه‌ی مجازی رفتار می‌کنند و دارای دو نقطه‌ی پایان، که



فرآیند کپسوله‌سازی بسته‌ی GRE

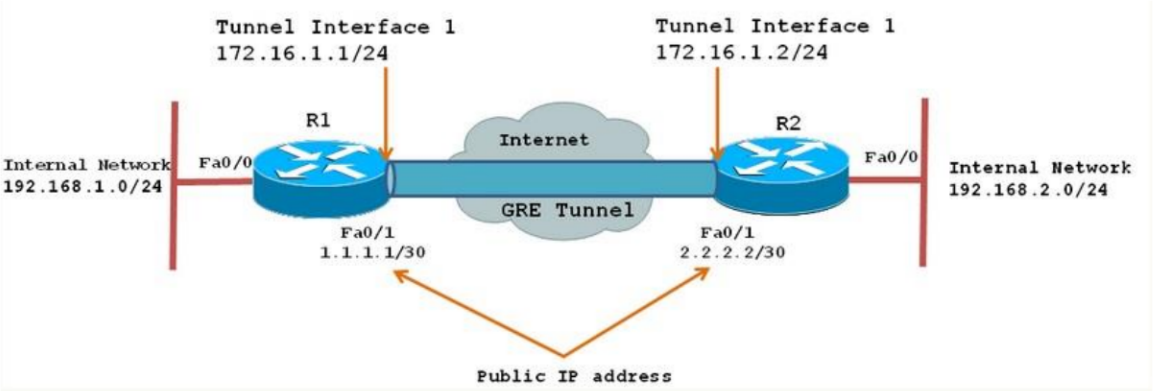
به‌وسیله‌ی آدرس‌های مبدا و مقصد تونل در هر نقطه‌ی پایان مشخص می‌شوند، هستند. تصویر زیر، فرایند کپسوله‌سازی بسته‌ی GRE را نشان می‌دهد که مسیریاب را می‌پیماید و وارد interface تونل می‌شود.

پیکربندی یک تونل GRE، شامل ساختن یک interface تونل بوده که یک interface منطقی است. سپس، باید نقاط پایان تونل را برای interface تونل پیکربندی نمود. برای پیکربندی مبدا و مقصد تونل باید از دستورات مبدا تونل {آدرس ip | نوع interface}، مقصد تونل {نام میزبان| آدرس ip}، و نیز دستورات تحت مد پیکربندی interface تونل استفاده نمود.

آزمایش شماره ۴

✓ سناریو آزمایش سوم

ابتدا نرم افزار GNS3 را از طریق سورس ارسال شده نصب و راه اندازی نمایید. سپس CISCO IOS 7200 را Mount کنید و از درستی نصب و راه اندازی روتر ۷۲۰۰ اطمینان حاصل نمایید. سپس توپولوژی زیر را در GNS3 بعنوان یک پروژه جدید و با نام شماره گروه خودتان ایجاد نمایید. در آزمایش زیر نحوه‌ی ساخت تونل‌های ساده‌ی GRE بین نقاط پایان و نیز، گام‌های اساسی برای ساخت و شناسایی تونل‌های GRE بین دو شبکه را ارایه شده است. مسیریاب‌های R1 و R2، متعلق به زیرشبکه‌های داخلی (192.168.1.0/24 و 192.168.2.0/24) بوده و در حال برقراری ارتباط با هر تونل GRE هستند که در اینترنت به‌کار می‌روند. هر دو interface تونل، جزئی از شبکه‌ی 172.16.1.0/24 هستند.



شبکه‌ی نمونه جهت پیکربندی تونل GRE

✓ روند کار

با فرض پیکربندی روتر ها و پیاده سازی مسیریابی OSPF، علاقه مند هستیم تا فرآیند چرخش بسته ها در شبکه واسط بین روترها را در GNS3 بررسی نماییم. پس از راه اندازی در فرآیند اجرا مراحل زیر را پایش کنید.

- ابتدا OSPF را در دو روتر راه اندازی نمایید. در شبکه های داخلی دو روتر در هر طرف یک VPC با آدرس IP در محدوده مشخص شده در شبکه داخلی قرار دهید. نشان دهید که در جداول مسیر یابی دو روتر همسایه ها بدرستی قابل رویت هستند و با پینگ کردن آدرس ها درستی نتایج را تایید