به نام خدا

دانشگاه تهران

پردیس فارابی

دانشکده مهندسی

گروه مهندسی کامپیوتر

دستور کار

آزمایشگاه شبکه‌های کامپیوتری

شماره

۶

پیکربندی و راه‌اندازی SSH

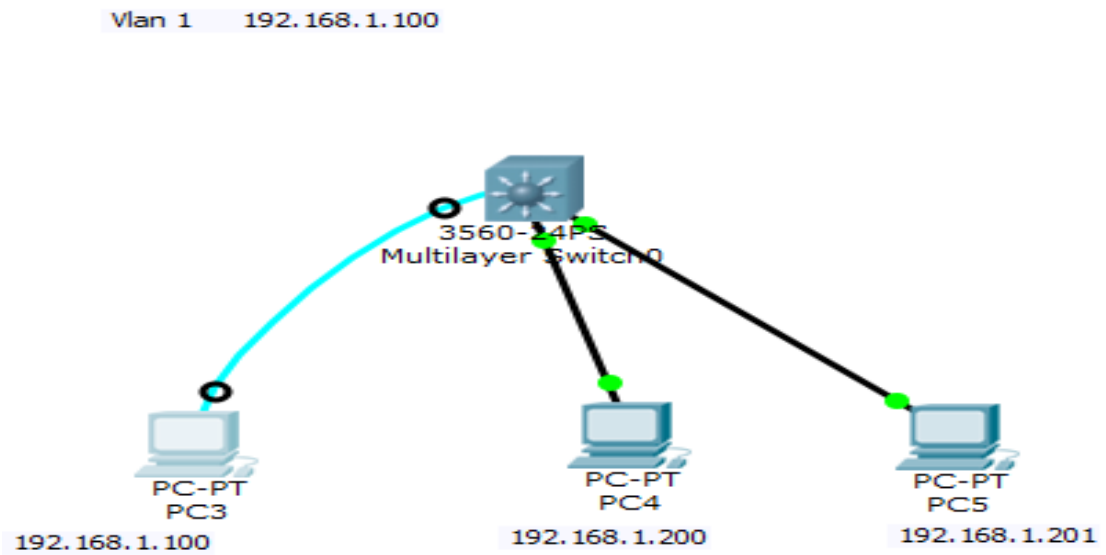
SSH Configuration and Setup

تا اینجا با config کردن device از طریق بستر IP آشنا شدیم. در شبکه‌های بزرگ بسته‌های ما از بسترهای مختلفی عبور می‌کنند. در telnet بسته‌های ارسالی به صورت clear text یا به عبارتی متن رمز نشده هستند و احتمال sniff شدن (استراق سمع) وجود دارد. درنتیجه از پروتکل دیگری به اسم SSH استفاده می‌شود که همان قابلیت telnet را به همراه امکان رمزنگاری بسته‌های ارسالی بین client/server برای ما فراهم می‌آورد.

نکته:IOS سوئیچ حتماً باید قابلیت رمزگذاری/ encryption داشته باشد وگرنه SSH را ساپورت نمی‌کند. اگر دستور `show ver` را در سوئیچ زدید و K9 بود، این قابلیت را دارد.

```
Switch#show version
Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version
12.2(37)SE1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 05-Jul-07 22:22 by pt_team
Image text-base: 0x00003000, data-base: 0x01500000

ROM: C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE SOFTWARE
(fc4)

System returned to ROM by power-on

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

در این سناریو یک سوئیچ 3560 قرار می‌دهیم و ابتدا برای تنظیمات اولیه، کامپیوتری را از طریق کابل کنسول به دستگاه وصل می‌کنیم و ssh را راه اندازی می‌نماییم. دو end device دیگر را نیز به سوئیچ وصل می‌کنیم، بر روی آن‌ها IP تنظیم می‌نماییم و داریم:



برای پیکربندی SSH:

۱. به سوئیچ IP می‌دهیم.

```
Switch#en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#ip address 192.168.1.100 255.255.255.0
```

برای اطمینان از برقرار بودن ارتباطات از کامپیوترهای موجود 192.168.1.100 را ping می‌کنیم.

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=64ms TTL=255
Reply from 192.168.1.100: bytes=32 time=0ms TTL=255
Reply from 192.168.1.100: bytes=32 time=0ms TTL=255
Reply from 192.168.1.100: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 64ms, Average = 16ms

PC>
```

۲. Line vty را امن می‌کنیم.

دقیقاً همانند Telnet می‌توان این لاین را امن کرد:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#username Network password test
Switch(config)#line vty 0 15
Switch(config-line)#login local
Switch(config-line)#exit
```

۳. Enable secret

```
Switch(config-line)#exit
Switch(config)#enable secret 123
```

۴. نام سوئیچ را عوض می‌کنیم (hostname).

```
Switch(config)#hostname Netlab
Netlab(config)#
```

۵. به سوئیچ نام دامنه می‌دهیم (Domain-name).

```
Netlab(config)#ip domain-name az.lab
```

۶. طول کلید encryption را افزایش می‌دهیم.

برای این‌که ارتباط میان device و pc ای که بر روی آن می‌خواهیم SSH بزنیم امن باشد، در بحث encryption از دو کلید استفاده می‌شود (رمزنگاری نامتقارن). هرچیزی که با public key رمز شود، با private key معادل آن باز می‌شود و بالعکس.

سوئیچ مربوطه یک public key و یک private key برای خود دارد، در هنگام اتصال یک کامپیوتر به آن سوئیچ، public key را در اختیار کامپیوتر قرار می‌دهد. کامپیوتر بسته‌های ارسالی خود را با آن کلید رمز و ارسال می‌کند و سوئیچ بسته‌ها را با private key خود باز می‌نماید.

```
Netlab(config)#crypto key generate rsa
The name for the keys will be: Netlab.az.lab
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Netlab(config)#
```

در اینجا طول کلید را می‌پرسد که ما در اینجا ۱۰۲۴ قرار داده‌ایم. هر چه این طول بیشتر باشد شکستن رمز سخت‌تر است.

می‌توان public key را دید:

```
Netlab#show crypto key mypubkey rsa
% Key pair was generated at: 0:59:53 UTC Mar 1 1993
Key name: Netlab.az.lab
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
 00007b39  00006ee6  00007062  0000419a  00004b5c  00007a88  0000799a
000040d6
 00001f3d  00002366  000045be  00006b6a  000048bf  00002866  00003a71
0000697d
 0000043d  00007604  00006d89  000027a2  000041cf  00005a8e  0000586d  4cac
% Key pair was generated at: 0:59:53 UTC Mar 1 1993
Key name: Netlab.az.lab.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
 000013c9  00004a93  00005ac1  000041c4  00006685  00004999  00005046
000000b8
 00006563  00004b0e  00003dfb  00001c96  0000310d  00001f81  00005a89
0000387a
 00004b00  00004212  000075dd  000060a4  00005a48  00001a27  00000417  79cd
Netlab#
```

این همان کلیدی است که باید در اختیار client قرار بگیرد.

telnet-server به‌صورت پیش‌فرض بر روی سوئیچ فعال است، اما ssh-server فعال نیست درصورتی‌که دستور زیر را اجرا کنیم، داریم:

```
Netlab>en
Netlab#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Netlab(config)#line vty 0 15
Netlab(config-line)#transport input ?
  all     All protocols
  none    No protocols
  ssh     TCP/IP SSH protocol
  telnet  TCP/IP Telnet protocol
```

به‌طور پیش‌فرض، telnet فعال است و برای فعال نمودن ssh باید مقابل این دستور ssh را قرار بدهیم. گزینه all جهت فعال نمودن هر دو حالت و none غیرفعال بودن هر دو حالت است.

```
Netlab(config-line)#transport input all
```

می‌توانیم مشخصات SSH را مشاهده کنیم:

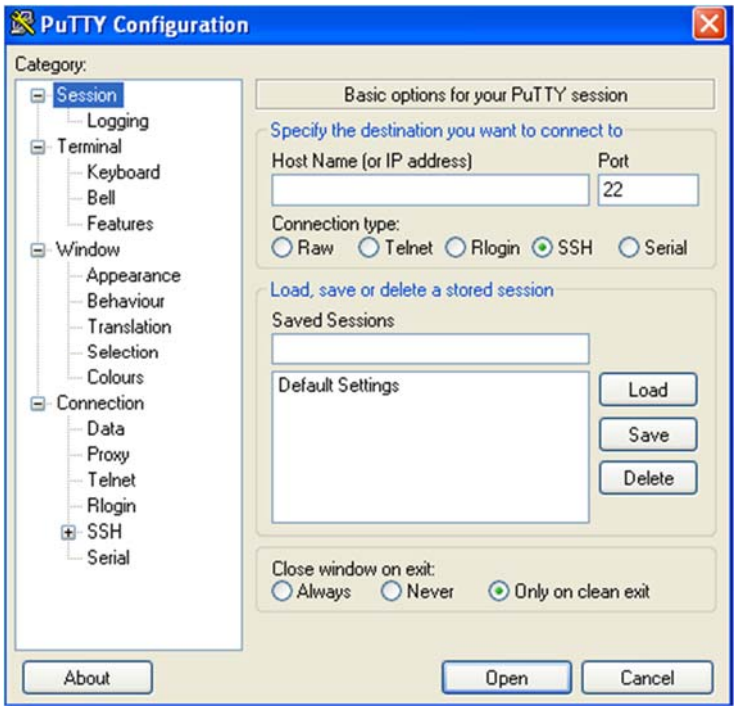
```
Netlab#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

این مقادیر پیش‌فرض را می‌توان تغییر داد. به‌عنوان مثال می‌توان تعداد دفعات تلاش برای authentication را به ۲ تغییر داد که این مقدار از ۰ تا ۵ قابل تغییر است و نیز می‌توان زمان برای صورت گرفتن atuthentication را به عنوان مثال ۶۰ قرار داد.

```
Netlab(config)#ip ssh ?
  authentication-retries  Specify number of authentication retries
  time-out                Specify SSH time-out interval
  version                 Specify protocol version to be supported
Netlab(config)#ip ssh aut
Netlab(config)#ip ssh authentication-retries 2
Netlab(config)#ip ssh time-out 60
Netlab(config)#do show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 60 secs; Authentication retries: 2
Netlab(config)#
```

تا به این‌جا ssh-server فعال شده است. کلاینت هم باید ssh-server را داشته باشد به طور پیش‌فرض ssh-server در ویندوز فعال نیست و از طریق applicationهایی مانند putty می‌توانیم یک ارتباط ssh و یک آدرس داشته باشیم.

برای اتصال ssh می‌توانید از نرم‌افزارهای جانبی مانند putty استفاده کنید.



در محیط Packet-Tracer برای تست ssh می‌توان بر روی کامپیوتری که قصد برقراری ارتباط ssh را داریم کلیک کنیم و در محیط command prompt دستور زیر را تایپ کنیم:

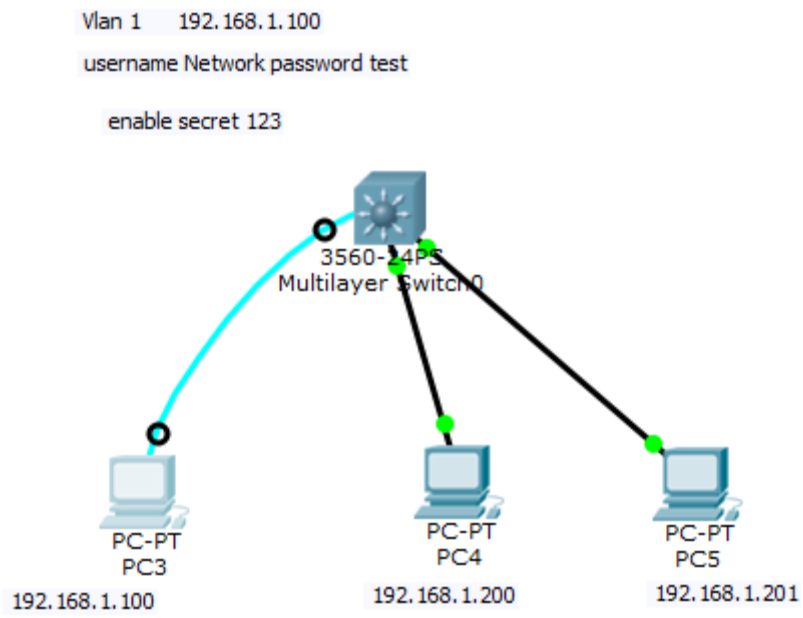
```
PC>ssh
Packet Tracer PC SSH

Usage: SSH -l username target
```

```
PC>ssh -l Network 192.168.1.100
Open
Password:



Netlab>
```

حال وارد مود enable می‌شویم:

```
Netlab>en
Password:
Netlab#
```

حال توانستیم به device، ssh بزنیم.



Banner

بنر/ Banner پیغامی است که توسط admin بر روی سوئیچ تنظیم می‌شود تا در هنگام ورود به نمایش گذاشته شود و در مود ۳ نوشته می‌شود.

بنر نباید اطلاعاتی در خصوص اینکه سوئیچ در کجا و چه استفاده‌ای دارد، بدهد و نباید تهدیدآمیز باشد.

بنرها براساس اینکه در کدام قسمت نمایش داده شوند انواع مختلفی دارند،

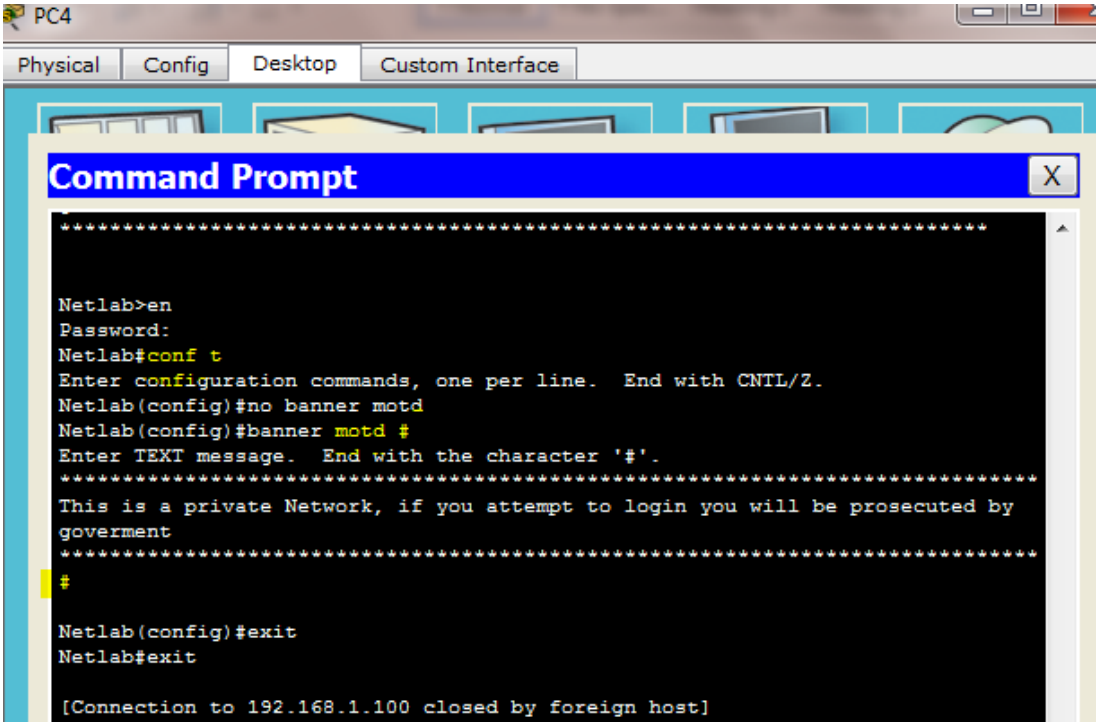
```
Netlab(config)#banner ?
  login  Set login banner
  motd   Set Message of the Day banner
```

Banner login در زمانی نمایش داده می‌شود که کاربر می‌خواهد به device وارد شود.

Banner motd پیامی را به‌صورت موقت ارسال می‌نماید و قبل از صفحه‌ی ورود به سوئیچ نمایش داده می‌شود.

می‌خواهیم از طریق ssh، banner را فعال نماییم:

نحوه‌ی استفاده از این دستور بدین‌صورت است که یک علامت که در متن قرار نیست از آن استفاده کنم، به کار می‌بریم و پس از آن متن و در انتها جهت خارج شدن از محیط text editor مجدداً علامت تعیین شده را می‌گذاریم.



حال show running-config را وارد می‌کنیم تا متوجه تغییرات شویم.

مجدداً از محیط خارج می‌شویم و دوباره وارد می‌شویم. مشاهده می‌کنیم که پیغام ظاهر می‌شود:

```
PC>ssh -l Network 192.168.1.100
Open
Password:


**********
This is a private Network, if you attempt to login you will be prosecuted by
goverment
**********


Netlab>
```

Login Time out

هنگام اتصال از طریق کنسول یا ریموت (telnet) اگر بعد از مدت زمانی فعالیتی انجام ندهیم از محیط خارج خواهیم شد.

این زمان را می‌توان تنظیم کرد، بهتر است نه خیلی کم و نه خیلی طولانی باشد (۳ دقیقه زمان خوبی است).

اگر به جای دقیقه و ثانیه هر دو را صفر بدهیم، این timer غیرفعال می‌شود.

```
Netlab>en
Password:
Netlab#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Netlab(config)#line console 0
Netlab(config-line)#exec-time دقیقه ثانیه
Netlab(config-line)#exit
Netlab(config)#line vty 0 15
Netlab(config-line)#exec-time دقیقه ثانیه
```