[MODULE 6]

Monitoring and Maintenance

Read Me

Ini adalah modul gratis, boleh digunakan oleh siapa saja untuk keperluan belajar (non-komersial) dan hal serupa lainnya tanpa menghapus footer credit dari webiptek.com.

Penjelasan dalam bentuk video (Bahasa Indonesia), silakan cek di Youtube:
https://www.youtube.com/playlist?list=PLnZp9Zjr0jNt84A7BFFUztsPILawYuIC0

by Rizqi Aldi Prayugo (xdnroot@gmail.com)

xdnroot
Last Update: 16/06/2020

Monitor Interface

root@router> **monitor interface** *<interface_name>*
Menampilkan jumlah paket dan ukuran paket yang melewati interface tersebut.

```
router                          Seconds: 8                    Time: 19:06:58
                                                             Delay: 0/0/1

Interface: em1, Enabled, Link is Up
Encapsulation: Ethernet, Speed: 1000mbps
Traffic statistics:                                        Current delta
  Input bytes:                 6201140                           [2046]
  Output bytes:                2826582                           [1666]
  Input packets:                 27518                             [21]
  Output packets:                21888                             [17]
Error statistics:
  Input errors:                      0                              [0]
  Input drops:                       0                              [0]
  Input framing errors:              0                              [0]
  Carrier transitions:               0                              [0]
  Output errors:                     0                              [0]
  Output drops:                      0                              [0]



Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'
```

Monitor Interface

root@router> **monitor interface traffic**

Menampilakan jumlah paket yang lewat di semua interface.

```
router                          Seconds: 50                 Time: 19:06:40

Interface    Link  Input packets        (pps)     Output packets        (pps)
 demux0        Up              0                             0
 dsc           Up              0                             0
 em0           Up          20012                         14889
 em1           Up          27472                         21850
 em2         Down              0                             0
 em3         Down              0                             0
 em4         Down              0                             0
 em5         Down              0                             0
 gre           Up              0                             0
 ipip          Up              0                             0
 irb           Up              0                             0
 lo0           Up             12                            12
 lsi           Up              0                             0
 mtun          Up              0                             0
 pimd          Up              0                             0
 pime          Up              0                             0
 pip0          Up              0                             0
 pp0           Up              0                             0


Bytes=b, Clear=c, Delta=d, Packets=p, Quit=q or ESC, Rate=r, Up=^U, Down=^D
```

Monitor Traffic

- Menampilkan detail traffic baik yang berasal maupun yang menuju perangkat.
- *monitor traffic* sama dengan *tcpdump* di linux (packet capturing).

root@router> **monitor traffic** *<option>*

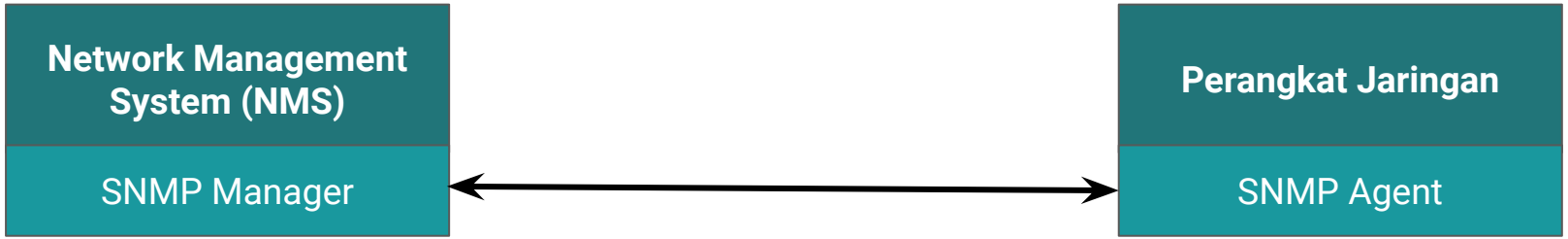
```
19:11:47.903485  In IP 192.168.1.2.37126 > 8.8.8.8.domain:  4676+ A? ntp.ubuntu.com. (32)
19:11:47.904221  In IP 192.168.1.2.58910 > 8.8.8.8.domain:  19698+ AAAA? ntp.ubuntu.com. (32)
19:11:49.594344  In IP truncated-ip - 256 bytes missing! 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Reques
t [|bootp]
19:11:52.906438  In IP 192.168.1.2.58910 > 8.8.8.8.domain:  19698+ AAAA? ntp.ubuntu.com. (32)
19:11:52.906965  In IP 192.168.1.2.37126 > 8.8.8.8.domain:  4676+ A? ntp.ubuntu.com. (32)
19:11:54.721280  In IP truncated-ip - 24 bytes missing! 192.168.1.2 > 192.168.1.1: ICMP echo request, id 3867, seq 1
, length 64
19:11:54.721794 Out IP truncated-ip - 24 bytes missing! 192.168.1.1 > 192.168.1.2: ICMP echo reply, id 3867, seq 1,
length 64
19:11:55.222513  In IP truncated-ip - 24 bytes missing! 192.168.1.2 > 192.168.1.1: ICMP echo request, id 3867, seq 2
, length 64
19:11:55.223060 Out IP truncated-ip - 24 bytes missing! 192.168.1.1 > 192.168.1.2: ICMP echo reply, id 3867, seq 2,
length 64
19:11:55.723542  In IP truncated-ip - 24 bytes missing! 192.168.1.2 > 192.168.1.1: ICMP echo request, id 3867, seq 3
, length 64
19:11:55.723849 Out IP truncated-ip - 24 bytes missing! 192.168.1.1 > 192.168.1.2: ICMP echo reply, id 3867, seq 3,
length 64
```

Monitor Traffic

```
root@router> monitor traffic ?
Possible completions:
  <[Enter]>             Execute this command
  absolute-sequence     Display absolute TCP sequence numbers
  brief                 Display brief output
  count                 Number of packets to receive (0..1000000 packets)
  detail                Display detailed output
  extensive             Display extensive output
  interface             Name of interface
  layer2-headers        Display link-level header on each dump line
  matching              Expression for headers of receive packets to match
  no-domain-names       Don't display domain portion of hostnames
  no-promiscuous        Don't put interface into promiscuous mode
  no-resolve            Don't attempt to print addresses symbolically
  no-timestamp          Don't print timestamp on each dump line
  print-ascii           Display packets in ASCII when displaying in hexadecimal format
  print-hex             Display packets in hexadecimal format
  resolve-timeout       Period of time to wait for each name resolution (seconds)
  size                  Amount of each packet to receive (bytes)
  |                     Pipe through a command
```

SNMP

SNMP merupakan protokol yang memberikan informasi terkait kondisi suatu perangkat, informasi ini digunakan untuk monitoring perangkat tersebut.
Informasi tersebut bisa berupa data statistik resources hardware, statistik traffic, dsb.



SNMP Basic Configuration

```
[edit snmp]
description "Junos Router";
location "Room 5, Rack 10B";
contact "rizqi@webiptek.com";
community public {
    authorization read-only;
    clients {
        192.168.1.0/24;
        10.1.1.1/24;
    }
}
trap-group public-trap {
    version v2;
    categories {
        chassis;
        link;
        routing;
    }
    targets {
        192.168.1.2;
    }
}
```

1. Informasi kontak.
2. Mendefinisikan community (minimal configuration).

   clients: adalah host (SNMP Manager) yang diizinkan untuk melakukan request snmp: get, getbulk, getnext.
3. Melakukan push informasi (notifications) kepada *targets (SNMP Manager)*.

Archiving Configuration Files

Menyimpan file konfigurasi di perangkat lain

```
[edit system archival]
configuration {
    transfer-on-commit;
    archive-sites {
        "ftp://user@10.10.2.5:/backup/config" password "$9$s.2JGjHqfQF"; ## SECRET-DATA
        "scp://user@192.168.1.2:/home/user/config" password "$9$0unzBhSlKMXNd"; ## SECRET-DATA
    }
}
```

metode pengarsipan konfigurasi dilakukan:

transfer-on-commit // archiving dilakukan ketika terjadi commit.

transfer-interval // archiving dilakukan setiap interval waktu tertentu (15-2880 menit).

archive-sites target perangkat untuk menyimpan file backup (archive), archiving bisa dilakukan menggunakan ssh dan ftp..

Delete Temporary Files.

```
# menampilkan temporary files yang akan dihapus.
root@vMX> request system storage cleanup dry-run

# menghapus temporary files.
root@vMX> request system storage cleanup
```

System Clean-up

```
# menghapus semua konfigurasi, log files dan menghapus keys values yang tersimpan.
root@router> request system zeroize
```

```
# menghapus semua konfigurasi dan menghapus keys values yang tersimpan, serta menghapus storage yang terhubung ke perangkat.
root@router> request system zeroize media
```

Upgrade or Downgrade the Junos OS

Jika perlu, download file image untuk upgrade/downgrade ke perangkat junos kita:

```
root@router> file copy <source-url-to-image> <destination-path>
# Contoh:
# root@router> file copy scp://10.1.1.2:/img/junos-vmx-x86-64-17.2R1.13.tgz /tmp/.
```

```
Untuk proses upgradenya gunakan command.
root@router> request system software add <path-to-image>
```

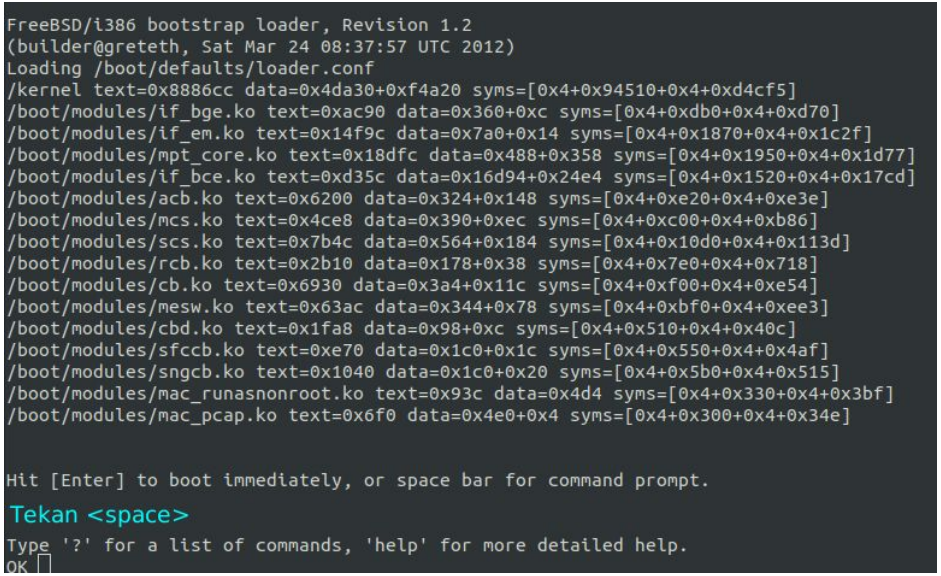
<path-to-image> bisa berupa path yang mengarah ke file image yang ada di local storage, bisa juga mengarah ke remote storage (ftp:// or scp://).

```
# Contoh:
# root@router> request system software add /tmp/junos-vmx-x86-64-17.2R1.13.tgz
```

Kemudian reboot.

Password Recovery

1. Reboot Junos OS.
2. Saat booting, masuk ke router's bootstrap loader mode dengan cara menekan tombol <space> pada saat muncul line:
   Hit [Enter] to boot immediately, or space bar for command prompt.



https://www.juniper.net/documentation/en_US/junos/topics/topic-map/recovering-root-password.html

Password Recovery

3. Boot ke single-user mode, dengan menjalankan command **boot -s**

```
Hit [Enter] to boot immediately, or space bar for command prompt.


Type '?' for a list of commands, 'help' for more detailed help.
OK boot -s
```

4. Masuk ke recovery mode.

```
Trying to mount root from ufs:/dev/ad0s1a
Attaching /packages/jbase via /dev/mdctl...
Mounted jbase package on /dev/md0...
System watchdog timer disabled
Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh: recovery
```

Password Recovery

5. Setelah CLI muncul, masuk ke configuration mode seperti biasa lalu lakukan reset password dengan perintah yang sama seperti mensetting root password.

```
root> configure

[edit]
root# set system root-authentication plain-text-password
New Password:
Retype New Password:

root# commit
```

6. Reboot dengan cara exit.

```
[edit]
root# exit
Exiting configuration mode

root> exit
Reboot the system? [y/n] y
```