EL5373

INTERNET ARCHITECTURE AND PROTOCOLS

Runze Dong

N10264442

rd1711@nyu.edu

Workstation: APAH Othello_I

MAC: f8:0f:41:c4:7f:aa

Lab Report 9

Exercise 1

1). The data type for the MIB object **ifMtu.2** is **Integer32**.

2). The **definition** of the MIB object **ifPhysAddress** and **ifInOctets**.
ifPhysAddress is The interface's address at its protocol sub-layer. For example, for an 802.x interface, this object normally contains a MAC address. The interface's media-specific MIB must define the bit and byte ordering and the format of the value of this object. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.
ifInOctets means the total number of octets received on the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

3). The data type and definition of **tcpRtoAlgorithm**
This **algorithm** used to determine the timeout value used for retransmitting unacknowledged octets. **Data type** is integer.

4). The **values allowed** for tcpRtoAlgorithm can be 1,2,3,4,5.

5). The definition of **tcpMaxConn**
TcpMaxConn is the limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

Exercise 2

1). What is the MTU of the Ethernet interface? What is the MTU of the loopback interface?
MTU of **Ethernet** Interface is **1500;** MTU of **Loopback** Interface is **65536**
And the result is same as the output of ifconfig command.

```
guest@othello1:~$ snmpwalk -v 2c -c guest localhost interface
Bad operator (INTEGER): At line 73 in /usr/share/mibs/ietf/SNMPv2-PDU
Unlinked OID in IPATM-IPMC-MIB: marsMIB ::= { mib-2 57 }
Undefined identifier: mib-2 near line 18 of /usr/share/mibs/ietf/IPATM-IPMC-MIB
Expected "::=" (RFC5644): At line 493 in /usr/share/mibs/iana/IANA-IPPM-METRICS-
REGISTRY-MIB
Expected "{" (EOF): At line 651 in /usr/share/mibs/iana/IANA-IPPM-METRICS-REGIST
RY-MIB
Bad object identifier: At line 651 in /usr/share/mibs/iana/IANA-IPPM-METRICS-REG
ISTRY-MIB
Bad parse of OBJECT-IDENTITY: At line 651 in /usr/share/mibs/iana/IANA-IPPM-METR
ICS-REGISTRY-MIB
IF-MIB::ifNumber.0 = INTEGER: 3
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifDescr.1 = STRING: lo
IF-MIB::ifDescr.2 = STRING: eth0
IF-MIB::ifDescr.3 = STRING: wlan0
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 65536
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifMtu.3 = INTEGER: 1500
```

2). Why did the snmpwalk command with a community name public fail?
The community name, public, is incorrect.
The "SNMP Community string" is like a user ID or password that allows access to a router's or other device's statistics. If the community string is incorrect, the device simply discards the request and does not respond.

Exercise 3

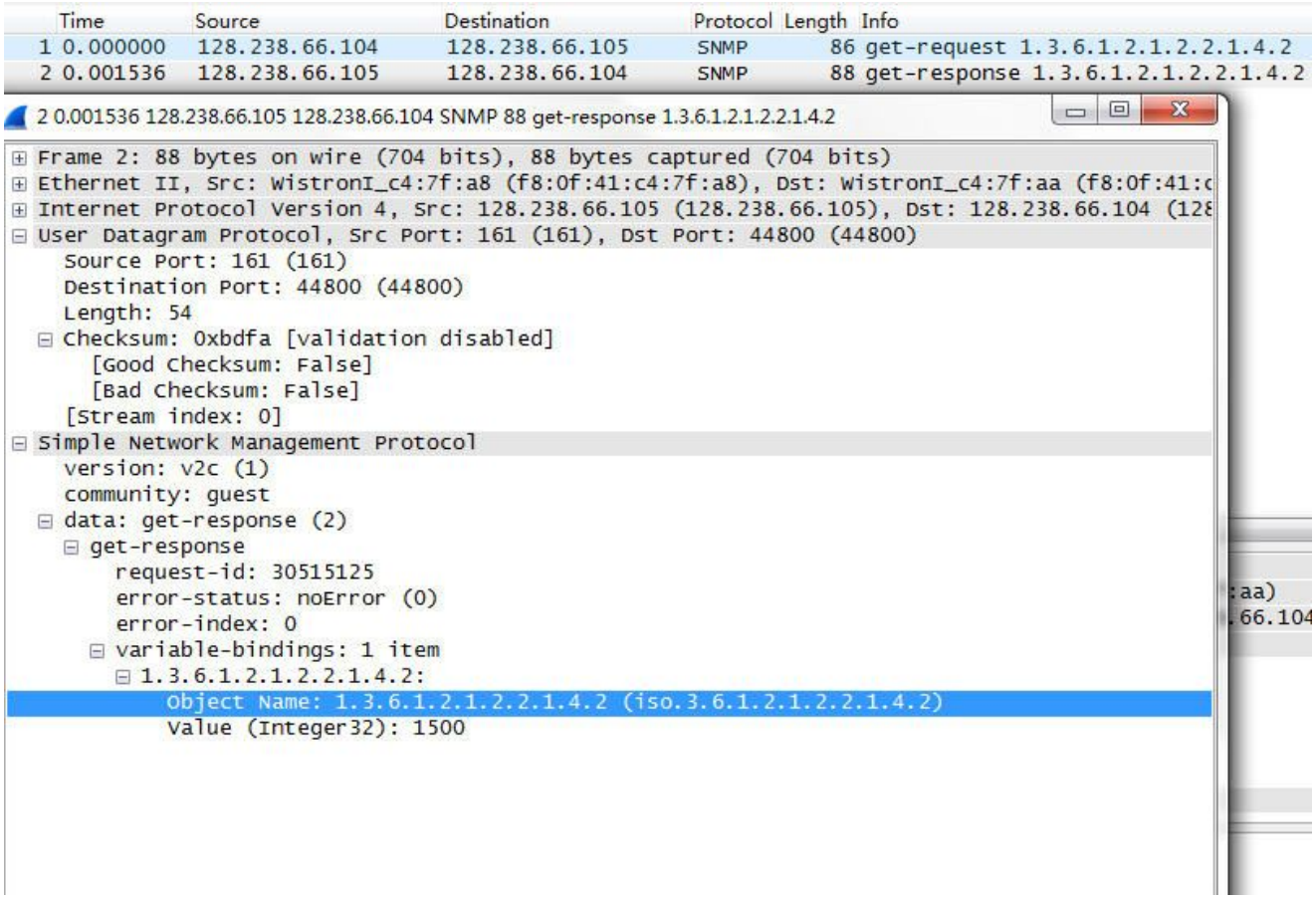
1). What is the port number used by the SNMP agent?
Port 161

2). What are the full text-based and numerical object ID's of the MIB objectinterface.ifMTU.2 ?
object name: 1.3.6.1.2.1.2.2.1.4.2 (iso.3.6.1.2.1.2.2.1.4.2)

3). What was the value returned? Justify the answer using Fig. 9.3 and the ifconfig output.
Value(Integer 32): 1500

4). Draw the format of one of the SNMP messages saved, including the name and value of each field.

Version Number	Community Name	PDU Type	Request ID	Error Status	Erroe Index	Object1	Value1
SNMP V2c	guest	get-response	30515125	noError(0)	0	1.3.6.1.2.1.2.2.1.4.2	1500



Exercise 4

1). Can you see the login ID and the password in the FTP experiment? Submit the packets that provide sufficient evidence.

Yes.

```
⊞ Frame 6: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
⊞ Ethernet II, Src: WistronI_c4:7f:aa (f8:0f:41:c4:7f:aa), Dst: WistronI_c4:7f:a8 (f8:0f:41:c
⊞ Internet Protocol Version 4, Src: 128.238.66.104 (128.238.66.104), Dst: 128.238.66.105 (128
⊞ Transmission Control Protocol, Src Port: 42040 (42040), Dst Port: 21 (21), Seq: 1, Ack: 21,
⊟ File Transfer Protocol (FTP)
  ⊟ USER 1111\r\n
      Request command: USER
      Request arg: 1111
```

```
10 5.564624 128.238.66.104 128.238.66.105 FTP 77 Request: PASS 2222
⊞ Frame 10: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
⊞ Ethernet II, Src: WistronI_c4:7f:aa (f8:0f:41:c4:7f:aa), Dst: WistronI_c4:7f:a8 (f8:0f:41:c
⊞ Internet Protocol Version 4, Src: 128.238.66.104 (128.238.66.104), Dst: 128.238.66.105 (128
⊞ Transmission Control Protocol, Src Port: 42040 (42040), Dst Port: 21 (21), Seq: 12, Ack: 55
⊟ File Transfer Protocol (FTP)
  ⊟ PASS 2222\r\n
      Request command: PASS
      Request arg: 2222
```

2). Can you see the login ID and the password in the TELNET experiment? Submit the packets that provide sufficient evidence.

Yes.we can find each character of the password and user name from telnet data packets.

```
17 0.059689 128.238.66.105 128.238.66.104 TELNET 84 Telnet Data ...
⊞ Frame 17: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
⊞ Ethernet II, Src: WistronI_c4:7f:a8 (f8:0f:41:c4:7f:a8), Dst: WistronI_c4:7f:aa (f8:0f:41:c
⊞ Internet Protocol Version 4, Src: 128.238.66.105 (128.238.66.105), Dst: 128.238.66.104 (128
⊞ Transmission Control Protocol, Src Port: 23 (23), Dst Port: 44171 (44171), Seq: 78, Ack: 11
⊟ Telnet
    Data: desdemona1 login:
```

```
23 7.446586 128.238.66.105 128.238.66.104 TELNET 67 Telnet Data ...
    [Calculated window size: 29056]
    [Window size scaling factor: 128]
  ⊞ Checksum: 0x4336 [validation disabled]
    Urgent pointer: 0
  ⊞ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ⊞ [SEQ/ACK analysis]
⊟ Telnet
    Data: 1
```

```
34 9.320352 128.238.66.105 128.238.66.104 TELNET 76 Telnet Data ...
⊞ Frame 34: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
⊞ Ethernet II, Src: WistronI_c4:7f:a8 (f8:0f:41:c4:7f:a8), Dst: WistronI_c4:7f:aa (f8:0f:41:c
⊞ Internet Protocol Version 4, Src: 128.238.66.105 (128.238.66.105), Dst: 128.238.66.104 (128
⊞ Transmission Control Protocol, Src Port: 23 (23), Dst Port: 44171 (44171), Seq: 102, Ack: 1
⊟ Telnet
    Data: Password:
```

```
38 10.645440 128.238.66.104 128.238.66.105 TELNET 67 Telnet Data ...
⊞ Frame 38: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
⊞ Ethernet II, Src: WistronI_c4:7f:aa (f8:0f:41:c4:7f:aa), Dst: WistronI_c4:7f:a8 (f8:0f:41:c
⊞ Internet Protocol Version 4, Src: 128.238.66.104 (128.238.66.104), Dst: 128.238.66.105 (128
⊞ Transmission Control Protocol, Src Port: 44171 (44171), Dst Port: 23 (23), Seq: 119, Ack: 1
⊟ Telnet
    Data: 2
```

3). What is the difference between FTP and TELNET in their transmission of user ID's and passwords? Is one more secure than the other and why?
For FTP, User's ID or password characters are transmitted directly in one whole packet.
For Telnet, They are transmitted as individual character one by one with several telnet data packets.
Telnet is more secure since the ID or password is divided into individual character and transmitted. But both of them didn't encode ID and password.

Exercise 5

1). Can you extract the password from the tcpdump output?
No. We can't extract the password because of SSH

2). Can you read the IP, TCP, SSH headers? Can you read and understand the TCP data?
Yes. All of the headers are accessible. But we can't read data.

```
⊟ Internet Protocol Version 4, Src: 128.238.66.104 (128.238.66.104), Dst: 128.238.66.105 (
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Ca
    Total Length: 572
    Identification: 0x4dd6 (19926)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
  ⊞ Header checksum: 0x6438 [validation disabled]
    Source: 128.238.66.104 (128.238.66.104)
    Destination: 128.238.66.105 (128.238.66.105)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Transmission Control Protocol, Src Port: 43728 (43728), Dst Port: 22 (22), Seq: 1490, Ack
    Source Port: 43728 (43728)
    Destination Port: 22 (22)
    [Stream index: 0]
    [TCP Segment Len: 520]
    Sequence number: 1490    (relative sequence number)
    [Next sequence number: 2010    (relative sequence number)]
    Acknowledgment number: 42    (relative ack number)
    Header Length: 32 bytes
  ⊞ .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    Window size value: 229
    [Calculated window size: 29312]
    [Window size scaling factor: 128]
  ⊞ Checksum: 0x88dc [unchecked, not all data available]
    Urgent pointer: 0
  ⊞ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ⊞ [SEQ/ACK analysis]
⊟ SSH Protocol
  ⊟ SSH Version 2
    ⊞ Packet Length: 1853059944
```

3). What is the client protocol (and version) used in both cases? What is the port number used by the ssh server? What is the port number used by the sftp server?
Both cases are used SSHv2. Both of them use port 22.

Exercise 8

1). Execute **iptables -L -v** to list the existing rules in the filter table.

```
guest@othello1: ~
guest@othello1:~$ iptables -L -v
modprobe: ERROR: could not insert 'ip_tables': Operation not permitted
iptables v1.4.21: can't initialize iptables table `filter': Table does not exist
 (do you need to insmod?)
Perhaps iptables or your kernel needs to be upgraded.
guest@othello1:~$ sudo iptable -L -v
[sudo] password for guest:
sudo: iptable: command not found
guest@othello1:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

guest@othello1:~$
```

2). Executing **iptables -A INPUT -v -p TCP ––dport 23 -j DROP**. Run **iptables -L -v** again to display the filter table.

```
guest@othello1:~$ iptables -A INPUT -v -p TCP --dport 23 -j DROP
iptables v1.4.21: can't initialize iptables table `filter': Permission denied (y
ou must be root)
Perhaps iptables or your kernel needs to be upgraded.
guest@othello1:~$ sudo iptables -A INPUT -v -p TCP --dport 23 -j DROP
DROP  tcp opt -- in * out *  0.0.0.0/0  -> 0.0.0.0/0   tcp dpt:23
guest@othello1:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 1 packets, 73 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 DROP       tcp  --  any    any     anywhere             anywhere
        tcp dpt:telnet

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

3). Can you telnet to the host from the remote machine? From the tcpdump output, how many retries did telnet make? Explain the exponential backoff algorithm of TCP timeout and retransmission.

We can't telnet to the host. TCP SYN request retries **6 times**.
For a TCP connection, there is at most one RTT measurement going on at any time instant. Since the measurements may have wide fluctuations due to transient congestion along the route, TCP uses a smoothed RTT, RT Ts, and the smoothed RTT mean deviation, RT Td, to compute the retransmission timeout (RTO) value. RTT measurement is not performed for a retransmitted TCP segment in order to avoid confusion, since it is not clear that if the received acknowledgement is for the original or the retransmitted segment. We use The Exponential Backoff algorithm to update RTO when the retransmission timer expires for a retransmitted segment. RTO is doubled for each retransmission, but with a maximum value of 64 seconds.

Exercise 9

1). Explain the difference between the tcpdump outputs of this exercise and the previous exercise. How many attempts did TCP make this time?
In this lab, client sends TCP SYN request and gets reset response. And then the connection is closed

```
1 0.000000   128.238.66.104   128.238.66.105   TCP   74 44237→23 [SYN] Seq=0 Win=
2 0.001034   128.238.66.105   128.238.66.104   TCP   60 23→44237 [RST, ACK] Seq=1

2 0.001034 128.238.66.105 128.238.66.104 TCP 60 23→44237 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  ⊟ .... 0000 0001 0100 = Flags: 0x014 (RST, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
    ⊞ .... .... .1.. = Reset: Set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
```

iptables -A INPUT -v -p TCP −−dport 23 -j DROP
iptables -A INPUT -v -p TCP −−dport 23 -j REJECT −−reject-with tcp-reset.
In exercise8, we use DROP option to discard any packets in port23 without sending any response to client. But in exercise9, we replace DROP with REJECT option. This means server not only rejects any packet in port 23 but sends a reset response to client. So when client gets a RESET flag packet, it will stop to retry.

Exercise 11

1). List the most frequently visited pages at the local Apache server and the remote Apache server during the most recent month, respectively.

Local Server, Othello_1 (104), I only get monthly statistics for May 2014. The most frequently visited page is /

Top 4 of 6 Total URLs					
#	Hits		kB F		URL
1	2	9.52%	1	5.67%	/
2	2	9.52%	1	7.76%	/try1.html
3	2	9.52%	1	7.50%	/try2.html
4	1	4.76%	1	8.23%	/webalizer/

Top 4 of 6 Total URLs By kB F					
#	Hits		kB F		URL
1	1	4.76%	1	8.23%	/webalizer/
2	2	9.52%	1	7.76%	/try1.html
3	2	9.52%	1	7.50%	/try2.html
4	2	9.52%	1	5.67%	/

Top 2 of 2 Total Entry Pages					
#	Hits		Visits		URL
1	2	9.52%	2	66.67%	/
2	1	4.76%	1	33.33%	/webalizer/

Top 1 of 1 Total Exit Pages					
#	Hits		Visits		URL
1	2	9.52%	2	100.00%	/try2.html

Remote Server, Petruchio_1 (106), I only get monthly statistics for Nov 2014.

The most frequently visited page is **/try1.html**

Top 3 of 5 Total URLs					
#	Hits		kB F		URL
1	9	19.15%	6	16.11%	/try1.html
2	4	8.51%	2	4.83%	/
3	3	6.38%	4	11.36%	/webalizer/

Top 3 of 5 Total URLs By kB F					
#	Hits		kB F		URL
1	9	19.15%	6	16.11%	/try1.html
2	3	6.38%	4	11.36%	/webalizer/
3	4	8.51%	2	4.83%	/

Top 3 of 3 Total Entry Pages					
#	Hits		Visits		URL
1	9	19.15%	3	42.86%	/try1.html
2	4	8.51%	2	28.57%	/
3	3	6.38%	2	28.57%	/webalizer/

Top 3 of 3 Total Exit Pages					
#	Hits		Visits		URL
1	4	8.51%	2	50.00%	/
2	9	19.15%	1	25.00%	/try1.html
3	3	6.38%	1	25.00%	/webalizer/

2). List the web pages that have the most number of bytes transferred by the local and the remote server during the most recent month, respectively.

Local Server, Othello_1 (104), the most number of bytes transferred is **/webalizer/**

Remote Server, Petruchio_1 (106),the most number of bytes transferred is **/try1.html**

Exercise 12

1). Is the rlogin service enabled in your host?
No. It's not enable.

Execute netstat -l

```
guest@othello1: ~
guest@othello1:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:time                  *:*                     LISTEN
tcp        0      0 othello1:domain         *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 *:39457                 *:*
udp        0      0 *:ipp                   *:*
udp        0      0 *:27773                 *:*
udp        0      0 *:mdns                  *:*
udp        0      0 *:time                  *:*
udp        0      0 othello1:domain         *:*
udp        0      0 *:bootpc                *:*
udp        0      0 *:tftp                  *:*
udp        0      0 172-27-222-251.DYNA:ntp *:*
udp        0      0 128.238.66.104:ntp      *:*
udp        0      0 localhost:ntp           *:*
udp        0      0 *:ntp                   *:*
udp        0      0 *:snmp                  *:*
udp6       0      0 [::]:45715              [::]:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:7606               [::]:*
udp6       0      0 fe80::fa0f:41ff:fec:ntp [::]:*
udp6       0      0 fe80::2c2:c6ff:fe7a:ntp [::]:*
udp6       0      0 ip6-localhost:ntp       [::]:*
udp6       0      0 [::]:ntp                [::]:*
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     30861    @guest-com.canonical.
Unity.Scope.scopes.T5944858777443
unix  2      [ ACC ]     STREAM     LISTENING     16536    @/tmp/.ICE-unix/2204
unix  2      [ ACC ]     STREAM     LISTENING     13181    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     44369    @/dbus-vfs-daemon/soc
ket-CrAtMyhE
unix  2      [ ACC ]     STREAM     LISTENING     16537    /tmp/.ICE-unix/2204
unix  2      [ ACC ]     STREAM     LISTENING     14863    /run/user/1000/keyrin
g-25KByj/control
```

Execute service --status-all

```
guest@othello1: ~
guest@othello1:~$ service --status -all
--status: unrecognized service
guest@othello1:~$ service --status-all
 [ + ]  acpid
 [ - ]  anacron
 [ + ]  apache2
 [ - ]  apparmor
 [ ? ]  apport
 [ + ]  avahi-daemon
 [ + ]  bluetooth
 [ - ]  brltty
 [ ? ]  console-setup
 [ + ]  cron
 [ + ]  cups
 [ + ]  cups-browsed
 [ - ]  dbus
 [ ? ]  dns-clean
 [ + ]  friendly-recovery
 [ - ]  grub-common
 [ ? ]  irqbalance
 [ + ]  kerneloops
 [ ? ]  killprocs
 [ ? ]  kmod
 [ ? ]  lightdm
 [ ? ]  networking
 [ + ]  ntp
 [ ? ]  ondemand
 [ - ]  openbsd-inetd
 [ ? ]  pppd-dns
 [ - ]  procps
 [ - ]  pulseaudio
 [ ? ]  rc.local
 [ + ]  resolvconf
 [ - ]  rsync
 [ + ]  rsyslog
 [ + ]  saned
 [ ? ]  sendsigs
 [ + ]  snmpd
 [ ? ]  speech-dispatcher
 [ - ]  ssh
 [ - ]  sudo
 [ - ]  tftpd-hpa
 [ - ]  udev
 [ ? ]  umountfs
 [ ? ]  umountnfs.sh
```