

Иногда бывает нужно проверить работы по SNMP с Linux. Сделать это можно через snmpwalk.

1. Установить snmpwalk можно так:

Для Ubuntu / Debian / Linux Mint

```
sudo apt-get update  
sudo apt-get install snmp
```

Проверка:

```
snmpwalk --version
```

Или для CentOS / RHEL / AlmaLinux / Rocky Linux (8 и выше)

```
sudo yum install net-snmp-utils
```

или

```
sudo dnf install net-snmp-utils
```

Проверка:

```
snmpwalk -h
```

2. Синтаксис следующий:

```
snmpwalk -v <версия> -c <community> <хост> <OID>
```

Расшифровка:

-v1/-v2c/-v3 - версия SNMP (1, 2c или 3)

-c <community> - ключ и указание community string (например, public), используется в SNMPv1/v2c

<хост> - IP-адрес или имя хоста устройства

<OID> - Объектный идентификатор (например, 1.3.6.1.2.1.1)

3. Примеры для -v1 и -v2c:

Получить всё

```
snmpwalk -v1 -c "public" 192.168.1.1 .1
```

Запрос всех данных из MIB-II (стандартная ветвь)

```
snmpwalk -v2c -c "public" 192.168.1.1 .1.3.6.1.2.1
```

Получить всё

```
snmpwalk -v2c -c "public" 192.168.1.1 .1
```

или по OID:

```
snmpwalk -v2c -c "public" 192.168.1.1 .1.3.6.1.2.1.1
```

4. Использование SNMPv3

Синтаксис:

```
snmpwalk -v3 -u <username> -l authPriv -a SHA -A <auth_password> -x AES -X  
<priv_password> 192.168.1.1 .1
```

Где:

- u – имя пользователя
- l – уровень безопасности: noAuthNoPriv, authNoPriv, authPriv
- a – алгоритм аутентификации (MD5, SHA)
- A – пароль аутентификации
- x – алгоритм шифрования (AES, DES)
- X – пароль шифрования

Пример с аутентификацией, но без шифрования трафика (authNoPriv):

```
snmpwalk -v3 -u myuser -l authNoPriv -a SHA -A "myAuthPassword123"  
192.168.1.1 .1
```

Тоже самое, но с MD5

```
snmpwalk -v3 -u myuser -l authNoPriv -a MD5 -A "myAuthPassword123"  
192.168.1.1 .1
```

Пример с аутентификацией и шифрованием трафика (authPriv):

```
snmpwalk -v3 -u myuser -l authPriv -a SHA -A "myAuthPassword123" -x AES -X  
myPrivPassword456 192.168.1.1 .1
```