PRILINK

http://www.prilink.com
Tel: 905-940-8844
Sales@prilink.com
Support@prilink.com

SIP-Trunk and Internet Monitor User Guide

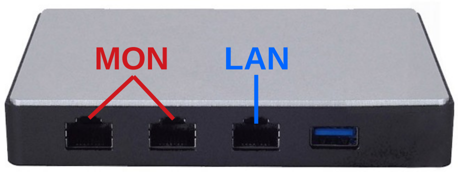
Table of Contents

Getting Started

This guide documents Prilink SIP-Trunk & Internet Monitor software version 2.3.5. For further assistance please contact Prilink support at 905-940-8844 or support@prilink.com.

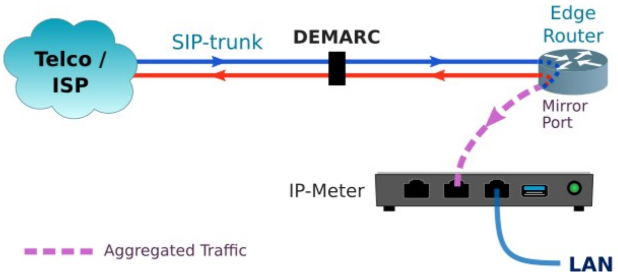
Hardware Setup

A Prilink **IP-Meter** collects and analyzes IP traffic data by monitoring 10/100/1000 Ethernet circuits through its monitor ports. A Mirror port or Ethernet TAP can be used to send a copy of network traffic from the DEMARC point to the IP-Meter monitor ports.

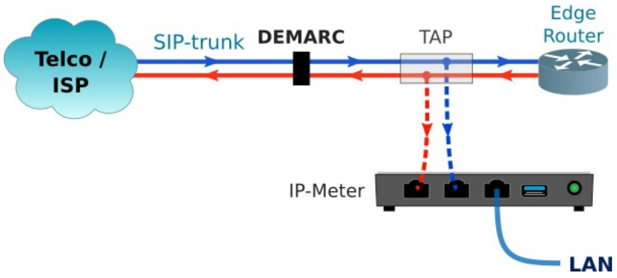


4.88” (124 mm) × 0.8” (21mm) × 4.7” (120mm)

Implementation using Mirror Port



Implementation using Network TAP



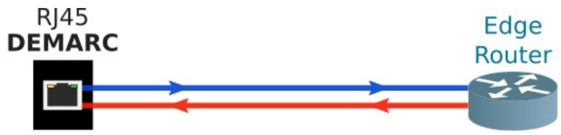
Implementation using Mirror Port

Before connecting power to the IP-Meter, first connect the LAN and monitor ports as follows:

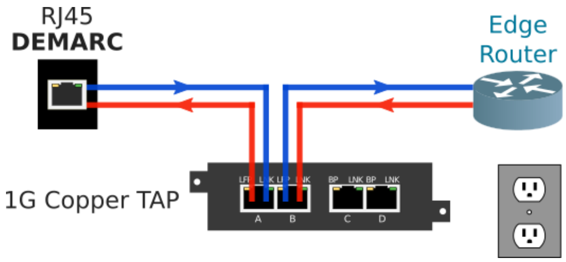
1. Connect the LAN port on the Meter to your network (the LAN port is labelled “LAN1”).
2. Configure port mirroring on your Switch/Server/Router.
3. Connect the monitor port on the Meter to the configured mirror port of your Switch/Server/Router (the monitor port is labelled “LAN2”).
4. Finally, connect power to the Meter.

Once powered on, wait approximately 2 minutes for the LED plug to begin blinking (the LED plug is the green RJ45 plug connected to the “Console” port).

Implementation using Network Tap

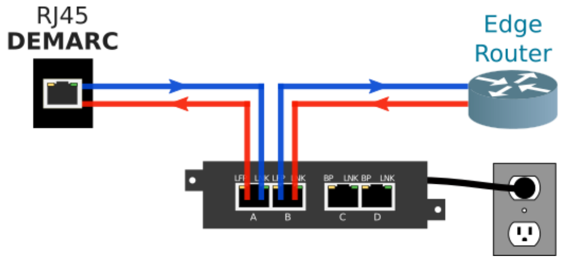


Step 1.



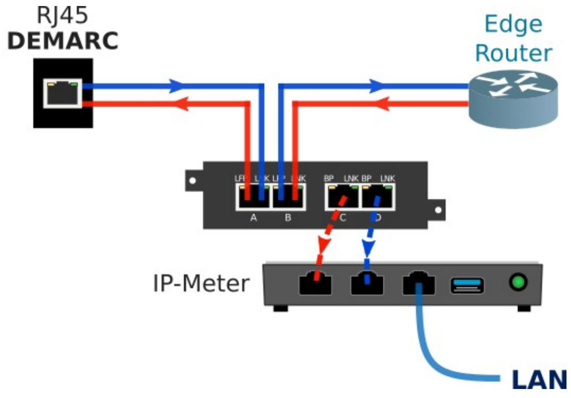
Connect Network TAP between **DEMARC** and Edge Router, without power connected to the TAP.

Step 2.



Connect power to Network TAP.

Step 3.



Connect monitor ports on IP-Meter to Network TAP.

Connect LAN port on IP-Meter to LAN.

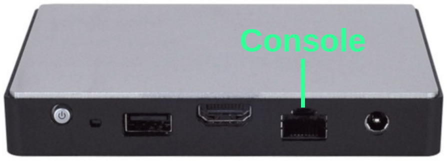
Connect power to IP-Meter.

Once the IP-Meter is powered on, wait approximately 2 minutes for the LED plug to begin blinking (the LED plug is the green RJ45 plug connected to the "Console" port).

IP Address Assignment

To configure the IP address settings on the IP Meter, establish a serial connection between the meter and your Windows PC as follows:

1. Locate the **Console Port** next to the DC jack. Remove the LED plug from the console port and connect the console port to your PC using console/serial cable.



2. Download the PuTTY terminal emulator:

   http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

3. Run **putty.exe** and configure the PuTTY menu as follows:

   a) Under **Connection type**, select *Serial*.

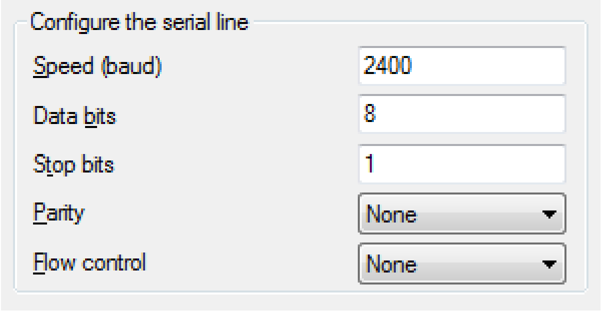
   b) In the **Serial line** field, enter the COM# you are using to connect your PC to the meter.

   c) In the **Speed** field, type *2400*.

   d) In the **Category** option tree on the left, choose *Connection* -> *Serial* and configure the serial line as shown on the right.

   e) Click **Open**.

   A blank screen should appear and the meter serial number should begin to output.


Configure the serial line

Speed (baud) 2400

Data bits 8

Stop bits 1

Parity None

Flow control None

4. Hit Enter to query the current IP address settings. The output will indicate whether the meter is using DHCP or a static IP address (**status** = 'dhcp' or 'static'). E.g.,

```
 status:  static a=192.168.0.30/24  g=192.168.0.1
```

5. To configure DHCP:

Type 'dhcp' and hit enter, then type 'y' and hit enter to confirm changes. The meter will reboot and attempt to acquire an IP address through DHCP.

5. To configure Static IP:

Type the following and hit enter, substituting desired values for *a* (address) and *g* (gateway):

```
 static a=192.168.0.2/24 g=192.168.0.1
```

(Note that *a* is written in CIDR notation: <**IP address**> / <**# of bits for routing prefix**>. To determine the number of bits for routing prefix based on a given netmask, see table below.) Type 'y' and hit enter to confirm changes. The meter will reboot with a static IP address.

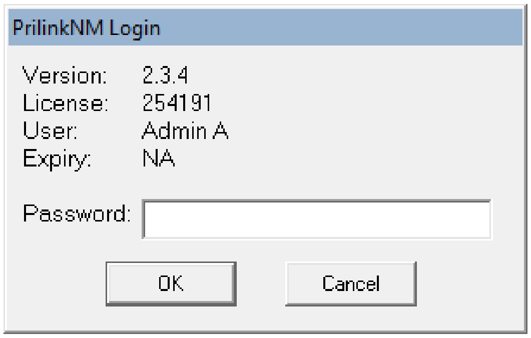
Table: Number of bits for routing prefix for a given netmask

Netmask	Prefix Bits	Netmask	Prefix Bits	Netmask	Prefix Bits	Netmask	Prefix Bits
128.0.0.0	1	255.128.0.0	9	255.255.128.0	17	255.255.255.128	25
192.0.0.0	2	255.192.0.0	10	255.255.192.0	18	255.255.255.192	26
224.0.0.0	3	255.224.0.0	11	255.255.224.0	19	255.255.255.224	27
240.0.0.0	4	255.240.0.0	12	255.255.240.0	20	255.255.255.240	28
248.0.0.0	5	255.248.0.0	13	255.255.248.0	21	255.255.255.248	29
252.0.0.0	6	255.252.0.0	14	255.255.252.0	22	255.255.255.252	30
254.0.0.0	7	255.254.0.0	15	255.255.254.0	23	255.255.255.254	31
255.0.0.0	8	255.255.0.0	16	255.255.255.0	24	255.255.255.255	32

6. Finally, disconnect the console/serial cable from the meter and replace the LED plug in the console port.

Software Setup

PrilinkNM application software can be installed on any Windows based PC or server by executing the **prilinknm-2.3.5-setup.exe** installer. Once installed, start the PrilinkNM application:


PrilinkNM Login

Version: 2.3.4
License: 254191
User: Admin A
Expiry: NA

Password:

You will be prompted for a password to begin. Enter the password that was supplied to you when you purchased the software.

If you have forgotten your password or do not have access to the installer, please contact Prilink support at 1-866-261-0649 or support@prilink.com.

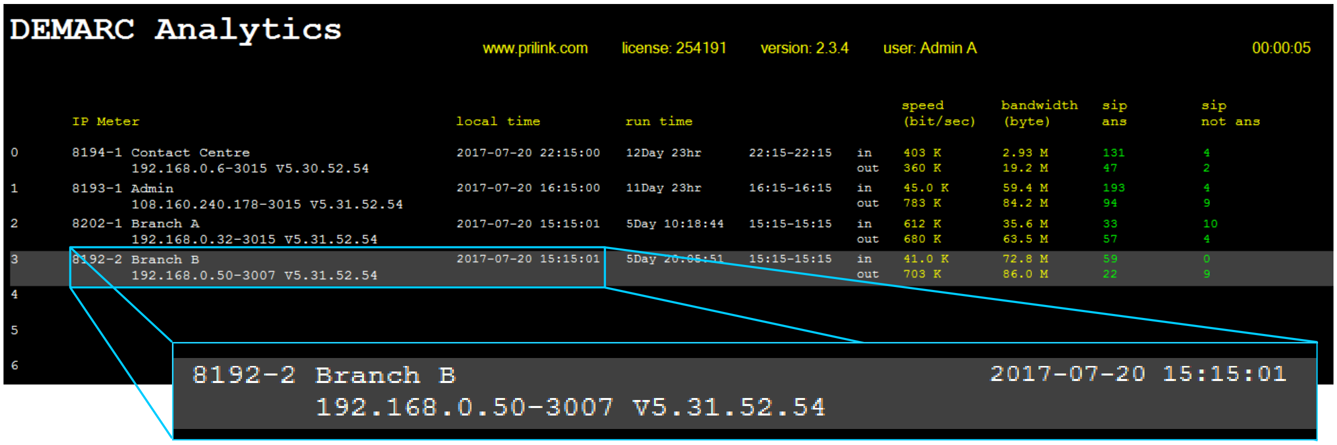
Keyboard navigation

The application can be navigated almost exclusively using the keyboard.

Arrow Keys or **PageUp** / **PageDown**	Highlight screen items or menu options one at a time (Arrow Keys) or one page at a time (PageUp / PageDown).
Enter	Access menu for selected screen item or choose menu option.
Esc	Go back to previous screen, close menu or exit application.

IP-Meter Connection Status

After successful login, the application will automatically attempt to connect to all IP-meters. When connected, the *local time* and *run time* fields will be populated and increasing.



```
DEMARC Analytics
                      www.prilink.com    license: 254191    version: 2.3.4    user: Admin A              00:00:05

                                                                                  speed       bandwidth  sip      sip
     IP Meter                                 local time           run time                                                (bit/sec)   (byte)     ans      not ans

0    8194-1 Contact Centre                    2017-07-20 22:15:00  12Day 23hr    22:15-22:15  in   403 K    2.93 M   131    4
            192.168.0.6-3015 V5.30.52.54                                                      out  360 K    19.2 M   47     2
1    8193-1 Admin                             2017-07-20 16:15:00  11Day 23hr    16:15-16:15  in   45.0 K   59.4 M   193    4
            108.160.240.178-3015 V5.31.52.54                                                  out  783 K    84.2 M   94     9
2    8202-1 Branch A                          2017-07-20 15:15:01  5Day 10:18:44 15:15-15:15  in   612 K    35.6 M   33     10
            192.168.0.32-3015 V5.31.52.54                                                     out  680 K    63.5 M   57     4
3    8192-2 Branch B                          2017-07-20 15:15:01  5Day 20:05:51 15:15-15:15  in   41.0 K   72.8 M   59     0
            192.168.0.50-3007 V5.31.52.54                                                     out  703 K    86.0 M   22     9
4

5

6
```

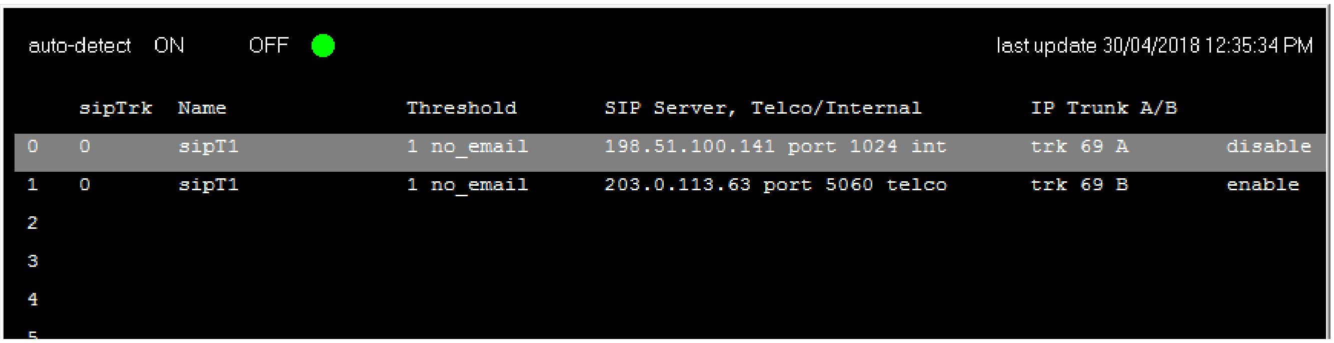
```
8192-2 Branch B                          2017-07-20 15:15:01
       192.168.0.50-3007 V5.31.52.54
```

If *local time* / *run time* fields are blank, the application is unable to connect to the IP-Meter. Check below the IP-Meter name to see which IP address/port the application is trying to reach the meter at (e.g. for IP-Meter 8192-2 above, it is 192.168.0.50 port 3007). If the address shown is not the same address that was assigned to the meter during installation, contact Prilink support for software update.

SIP Trunk Table

In order to compile SIP trunk analytics, an IP-Meter must know where to look for SIP signalling. The main purpose of the **SIP Trunk Table** is to tell the IP-Meter which IP addresses and port numbers are used for SIP signalling. The table is also used to assign names to SIP trunks, and to identify which IP addresses are Telco-side, so that the direction of SIP calls can be recorded correctly.

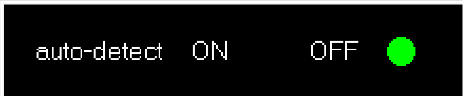
To view or edit the SIP Trunk Table, highlight an IP-Meter on the main screen, hit Enter and choose menu option *SIP Trunk*:



```
auto-detect  ON     OFF ●                                                 last update 30/04/2018 12:35:34 PM

    sipTrk  Name             Threshold         SIP Server, Telco/Internal           IP Trunk A/B
0   0       sipT1            1 no_email        198.51.100.141 port 1024 int         trk 69 A          disable
1   0       sipT1            1 no_email        203.0.113.63 port 5060 telco         trk 69 B          enable
2
3
4
5
```

SIP trunks can be detected automatically by the IP-Meter or defined manually.

Auto-Detect



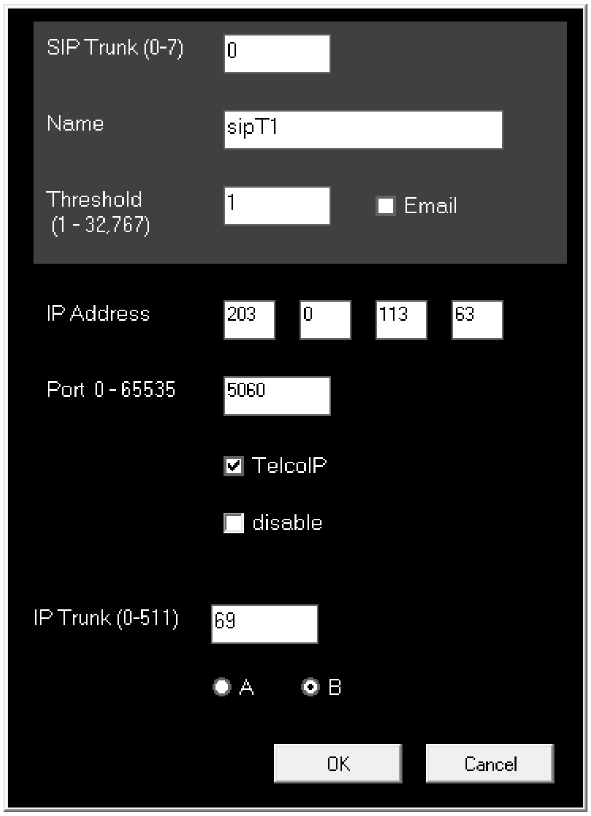
auto-detect ON OFF ●

When SIP trunk auto-detection is turned on, the IP-Meter will scan all packets for SIP signalling. When a SIP packet is detected, the meter will check if the packet matches any current entries in the SIP Trunk Table. If there is no match, it will create new entries based on the SIP packet, and auto-detection will be turned off.

Auto-detection can be turned on again by hitting Enter and choosing menu option *Detect On*. Once all SIP Trunks have been detected, auto-detection should remain off to conserve IP-Meter resources.

Manual Edit

To edit an existing entry in the SIP Trunk Table, or to create a new entry, highlight a row, hit Enter and choose menu option *Edit*:



SIP Trunk (0-7) 0

Name sipT1

Threshold (1 - 32,767) 1 □ Email

IP Address 203 0 113 63

Port 0 - 65535 5060

☑ TelcoIP

□ disable

IP Trunk (0-511) 69

○ A ● B

SIP Trunk: Number from 0–7 identifying this SIP trunk (up to 8 SIP trunks can be defined). Multiple entries can be combined by using the same SIP Trunk number (for example, if you want to group SIP traffic from multiple IP addresses)

Name: Any meaningful name for this SIP trunk.

Threshold: Number of active channels that must be reached in order to generate an alert (see Alerts).

IP address: IP address used for SIP signalling.

Port: TCP/UDP port number used by the above IP address for SIP signalling.

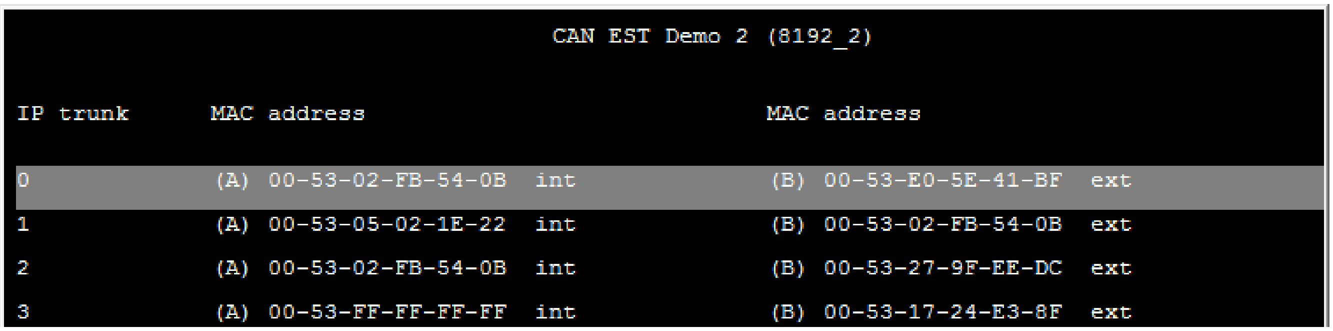
TelcoIP: Is the above IP address on the Telco side? This is used to categorize calls as inbound vs outbound.

disable: Check this field to ignore this entry.

IP Trunk: See IP Trunk Table below.

IP Trunk Table

An *IP trunk* is a pair of MAC addresses that have exchanged network traffic. The IP-Meter automatically detects and compiles network analytics on each unique IP trunk. To view all IP trunks detected (the **IP Trunk Table**), highlight an IP-Meter from the main screen, hit Enter and choose menu option *IP Trunk.*



```
                               CAN EST Demo 2 (8192_2)

IP trunk       MAC address                             MAC address

0               (A)  00-53-02-FB-54-0B  int            (B)  00-53-E0-5E-41-BF  ext
1               (A)  00-53-05-02-1E-22  int            (B)  00-53-02-FB-54-0B  ext
2               (A)  00-53-02-FB-54-0B  int            (B)  00-53-27-9F-EE-DC  ext
3               (A)  00-53-FF-FF-FF-FF  int            (B)  00-53-17-24-E3-8F  ext
```

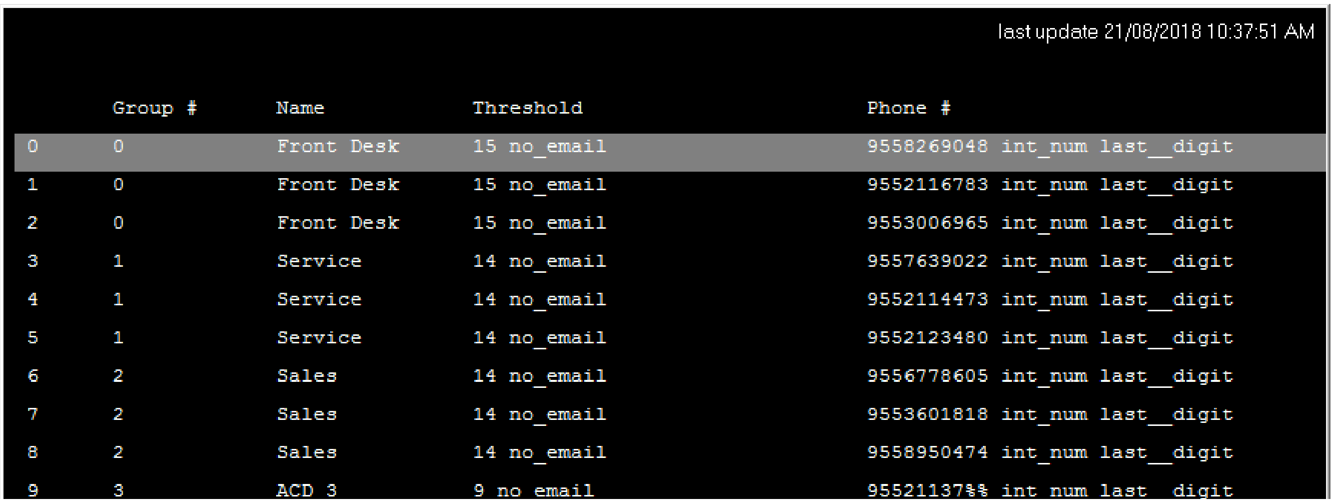
IP trunks are numbered starting from 0. When an IP trunk is first detected, the IP-Meter will arbitrarily label the MAC addresses “**A**” and “**B**”, based on the source and destination of the first packet received. For example, in IP trunk #2 above, the “A” side is `00-53-02-FB-54-0B` and the “B” side is `00-53-27-9F-EE-DC`.

When defining a SIP trunk in the SIP Trunk Table, in addition to specifying the IP address and port number used for SIP signalling, you must also specify the IP trunk used and the side of the IP trunk (A or B) where the specified IP address will be found.

SIP Group / Route Table

Once SIP trunks have been defined, the IP-Meter will automatically detect all internal and external SIP endpoints (phone numbers) and will compile network analytics on each individual phone number. A *SIP group* is a combination of phone numbers that you wish to monitor as a unit, such as a route, ACD queue, or other important business application.

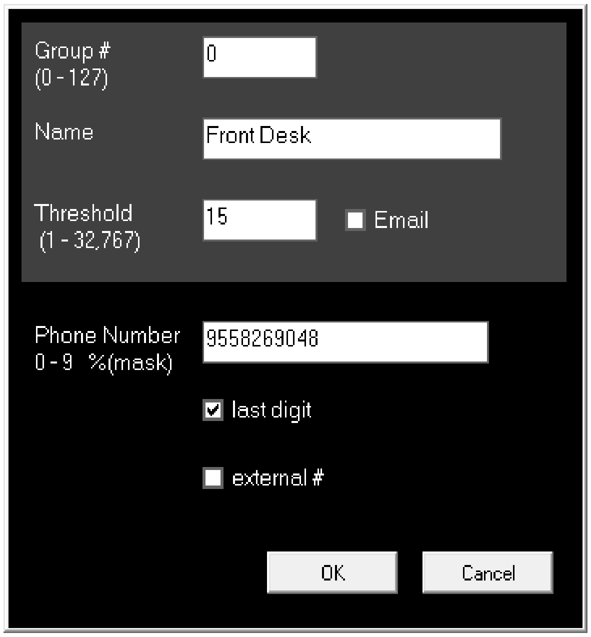
The **SIP Group Table** allows up to 128 SIP groups to be defined. To view or edit the SIP Group Table, highlight an IP-Meter on the main screen, hit Enter and choose menu option *SIP Group*:



```
                                                                last update 21/08/2018 10:37:51 AM

        Group #      Name            Threshold                      Phone #
 0      0            Front Desk      15 no_email                    9558269048 int_num last__digit
 1      0            Front Desk      15 no_email                    9552116783 int_num last__digit
 2      0            Front Desk      15 no_email                    9553006965 int_num last__digit
 3      1            Service         14 no_email                    9557639022 int_num last__digit
 4      1            Service         14 no_email                    9552114473 int_num last__digit
 5      1            Service         14 no_email                    9552123480 int_num last__digit
 6      2            Sales           14 no_email                    9556778605 int_num last__digit
 7      2            Sales           14 no_email                    9553601818 int_num last__digit
 8      2            Sales           14 no_email                    9558950474 int_num last__digit
 9      3            ACD 3           9 no_email                     95521137%% int_num last__digit
```

Each SIP Group is defined by one or more entries in the SIP Group Table. For example, Group #0 above (“Front Desk”) is defined by three entries, combining three internal phone numbers.

To edit an existing entry, or to create a new entry, highlight a row, hit Enter and choose menu option *Edit*:



Group # (0 - 127): 0

Name: Front Desk

Threshold (1 - 32,767): 15 □ Email

Phone Number 0 - 9 %(mask): 9558269048

☑ last digit

□ external #

Group #: Number from 0–127 identifying this SIP group (up to 128 groups can be defined). Multiple entries can be combined by using the same Group #.

Name: Any meaningful name for this SIP group.

Threshold: Number of active channels that must be reached in order to generate an alert (see Alerts).

Phone Number: Phone number to match. The % character can be used as a wildcard to match any digit. If the **last digit** field is checked, then any phone number whose last digits are equal to the above number will be included in the group. Otherwise, an exact match is required to be included.

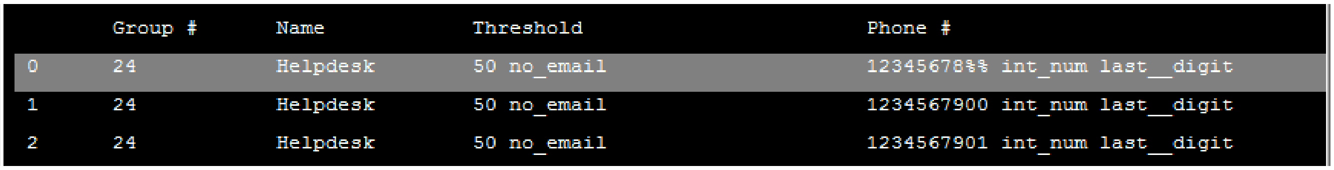
External #: Is this an external phone number?

SIP Group Example: Help Desk

Suppose our Help Desk includes 12 internal phone numbers:

123-456-7800	123-456-7803	123-456-7806	123-456-7809
123-456-7801	123-456-7804	123-456-7807	123-456-7900
123-456-7802	123-456-7805	123-456-7808	123-456-7901

Suppose further that for outbound calls, the phone numbers appear prefixed by 1 (eg. 1-123-456-7800). By checking **last digit** in each group entry, we can ensure that both outbound and inbound calls are matched. The complete group definition would require only 3 entries:

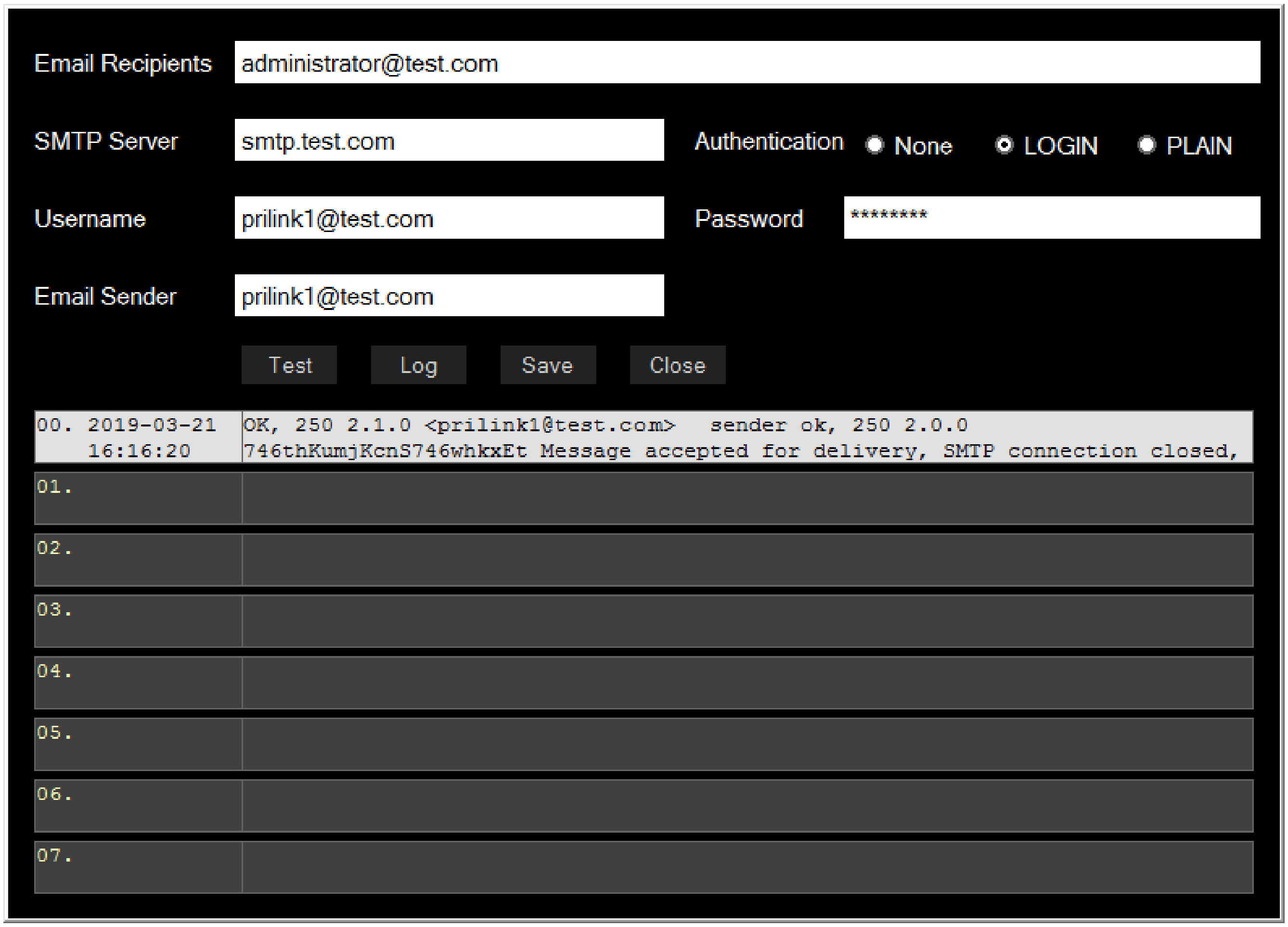


```
      Group #    Name        Threshold               Phone #
0     24         Helpdesk    50 no_email             12345678%% int_num last__digit
1     24         Helpdesk    50 no_email             1234567900 int_num last__digit
2     24         Helpdesk    50 no_email             1234567901 int_num last__digit
```

Alert Notifications

In both the SIP Trunk Table and SIP Group Table, each SIP trunk or group can be assigned a channel *threshold*. If the number of active calls belonging to the trunk / group ever reaches the assigned threshold, then an alert is generated. The SIP trunk / group definition dialog includes an **email** checkbox that should be checked if you wish to receive notifications by email for threshold alerts. A maximum of 3 alerts per 15 minutes will be generated for each SIP trunk or group.

In order for Email notification to function, the PrilinkNM application must be able to connect to an outgoing SMTP mail server. To configure mail server settings, hit Enter from the main screen and choose menu option *Email*:



Email Recipients: administrator@test.com

SMTP Server: smtp.test.com

Authentication: ○ None ● LOGIN ○ PLAIN

Username: prilink1@test.com

Password: *********

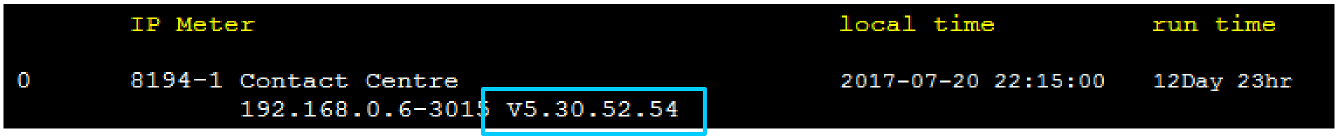
Email Sender: prilink1@test.com

```
00. 2019-03-21  OK, 250 2.1.0 <prilink1@test.com>   sender ok, 250 2.0.0
    16:16:20    746thKumjKcnS746whkxEt Message accepted for delivery, SMTP connection closed,
01.
02.
03.
04.
05.
06.
07.
```

Use the *Test* button to send a test message, and consult the *Log* to see the response from your mail server. Hit *Save* to store mail server settings permanently, or hit *Close* to return to previous settings.

Firmware Updates

The firmware version running on an IP-Meter can be viewed at any time from the main screen:



```
        IP Meter                                              local time           run time

0       8194-1 Contact Centre                                 2017-07-20 22:15:00  12Day 23hr
               192.168.0.6-3015 v5.30.52.54
```

The version string is composed of “Server” version followed by “Site” version. For example, `v5.30.52.24` indicates Server version `5.30` and Site version `52.54`.

Firmware updates are completed using the PrilinkNM application as follows:

1. Extract firmware files into `C:\ip` directory.
2. Highlight IP-Meter on the main screen, hit Enter and choose menu option *Server Reboot/Shutdown/Update*. Then choose sub-option *Firmware Update*.
3. Wait approximately 2 minutes while the IP-Meter reboots. Once the application reconnects to the IP-Meter, confirm that Server version has updated (first half of version string).
4. Highlight IP-Meter on the main screen, hit Enter and choose menu option *Site Reboot/Shutdown/Update*. Then choose sub-option *Firmware Update*.
5. Wait approximately 2 minutes while the IP-Meter reboots. Once the application reconnects to the IP-Meter, confirm that Site version has updated (second half of version string).

Firmware update is complete.

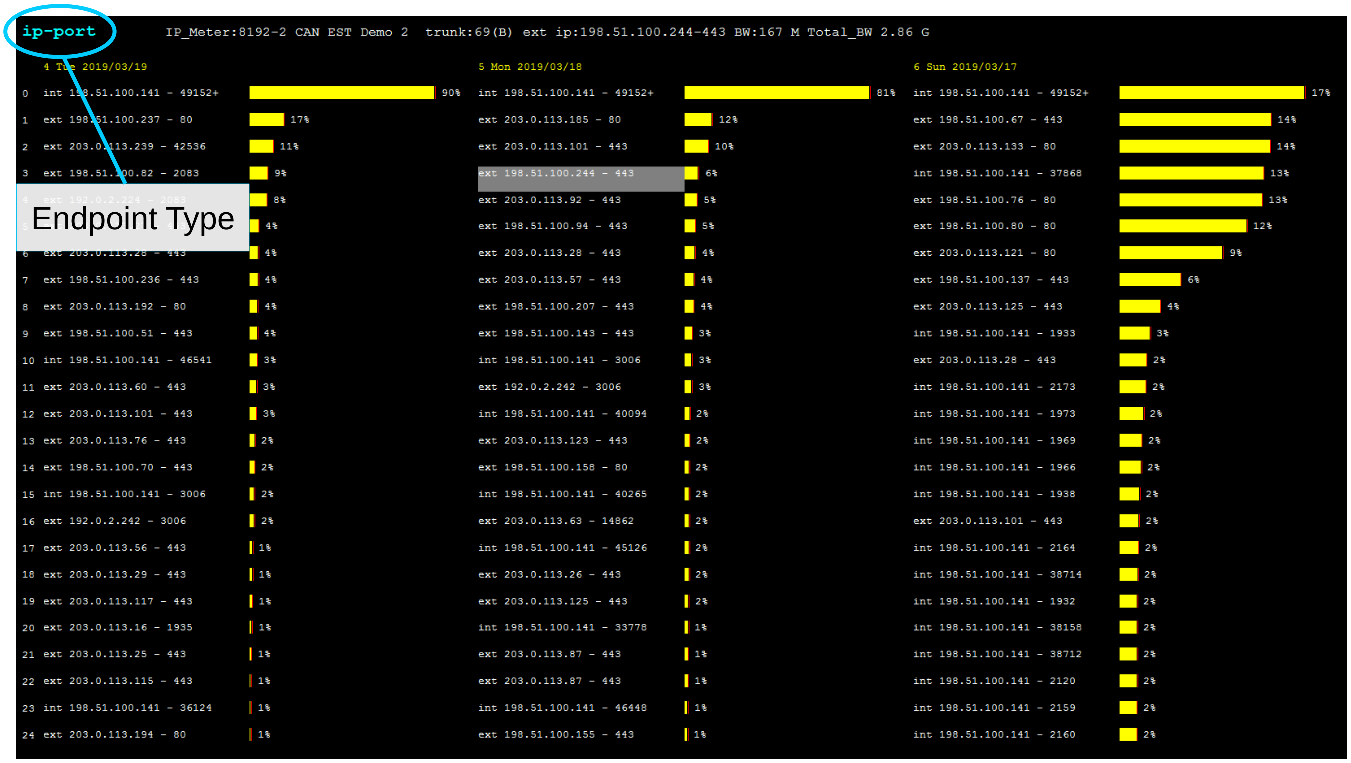
Exploring Network Endpoint Analytics

The IP-Meter automatically scans several types of network endpoints at the Link, Internet, Transport and Application layers, and compiles network analytics for each endpoint. There are 6 endpoint types:

SIP Number	SIP Phone Number
SIP Trunk	SIP Trunk as defined in the SIP Trunk Table
IP – Port	Combination of IP address and transport layer port number
IP	IP address
EtherType	EtherType number indicating protocol (IPv4, IPv6, ARP, etc...)
IP Trunk	Pair of MAC Addresses that have exchanged network traffic (see IP Trunk Table)

Active Endpoint

The IP-Meter continuously monitors and sorts the most active endpoints of each type. To browse the top endpoints over the last 500 days, highlight an IP-Meter from the main screen, hit Enter and choose menu option *Active Endpoint*:

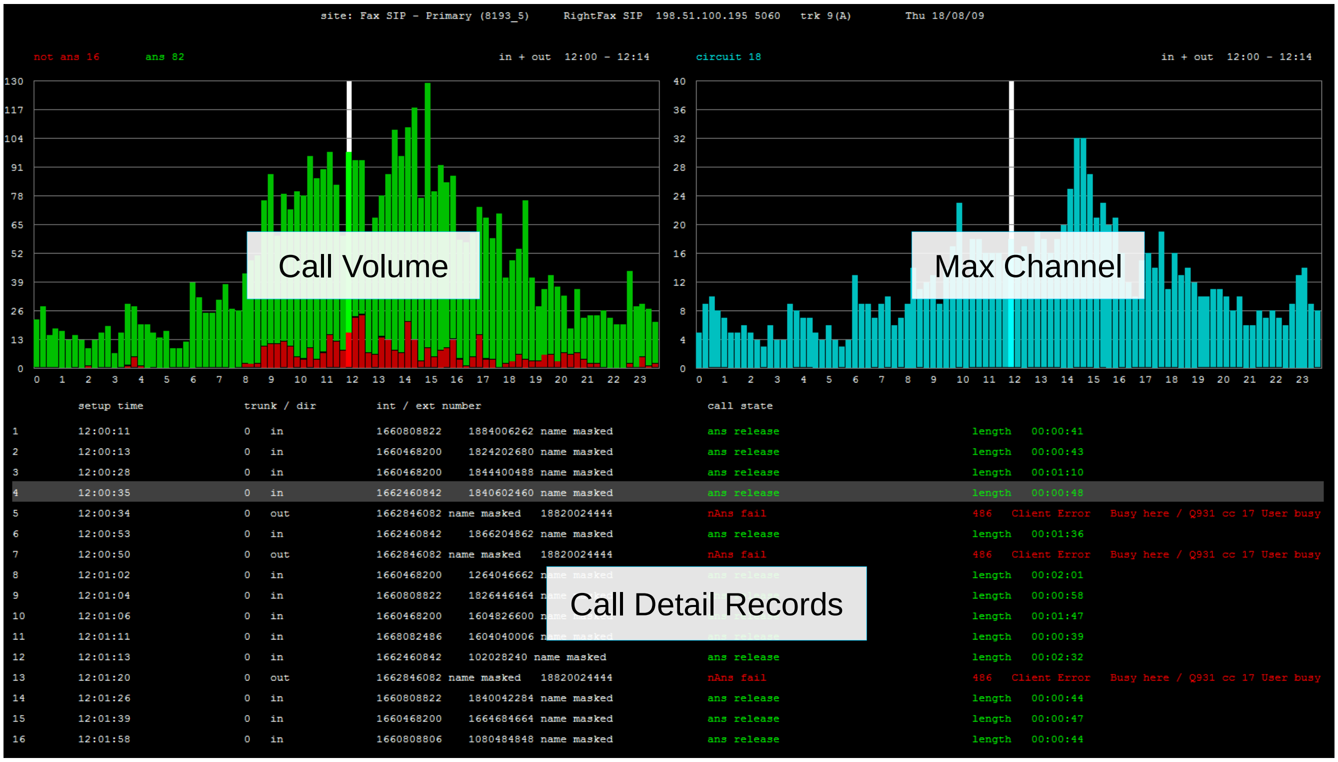


```
ip-port       IP_Meter:8192-2 CAN EST Demo 2  trunk:69(B) ext ip:198.51.100.244-443 BW:167 M Total_BW 2.86 G

   4 Tue 2019/03/19                        5 Mon 2019/03/18                        6 Sun 2019/03/17
0  int 198.51.100.141 - 49152+  90%   int 198.51.100.141 - 49152+  81%   int 198.51.100.141 - 49152+  17%
1  ext 198.51.100.237 - 80      17%   ext 203.0.113.185 - 80       12%   ext 198.51.100.67 - 443      14%
2  ext 203.0.113.239 - 42536    11%   ext 203.0.113.101 - 443      10%   ext 203.0.113.133 - 80       14%
3  ext 198.51.100.82 - 2083      9%   ext 198.51.100.244 - 443      6%   int 198.51.100.141 - 37868   13%
4  ext 192.0.2.224 - 2083        8%   ext 203.0.113.92 - 443        5%   ext 198.51.100.76 - 80       13%
5  ext 203.0.113.2[illegible] - 443     4%   ext 198.51.100.94 - 443       5%   ext 198.51.100.80 - 80       12%
6  ext 203.0.113.28 - 443        4%   ext 203.0.113.28 - 443        4%   ext 203.0.113.121 - 80        9%
7  ext 198.51.100.236 - 443      4%   ext 203.0.113.57 - 443        4%   ext 198.51.100.137 - 443      6%
8  ext 203.0.113.192 - 80        4%   ext 198.51.100.207 - 443      4%   ext 203.0.113.125 - 443       4%
9  ext 198.51.100.51 - 443       4%   ext 198.51.100.143 - 443      3%   int 198.51.100.141 - 1933     3%
10 int 198.51.100.141 - 46541    3%   int 198.51.100.141 - 3006     3%   ext 203.0.113.28 - 443        2%
11 ext 203.0.113.60 - 443        3%   ext 192.0.2.242 - 3006        3%   int 198.51.100.141 - 2173     2%
12 ext 203.0.113.101 - 443       3%   int 198.51.100.141 - 40094    2%   int 198.51.100.141 - 1973     2%
13 ext 203.0.113.76 - 443        2%   ext 203.0.113.123 - 443       2%   int 198.51.100.141 - 1969     2%
14 ext 198.51.100.70 - 443       2%   ext 198.51.100.158 - 80       2%   int 198.51.100.141 - 1966     2%
15 int 198.51.100.141 - 3006     2%   int 198.51.100.141 - 40265    2%   int 198.51.100.141 - 1938     2%
16 ext 192.0.2.242 - 3006        2%   ext 203.0.113.63 - 14862      2%   ext 203.0.113.101 - 443       2%
17 ext 203.0.113.56 - 443        1%   int 198.51.100.141 - 45126    2%   int 198.51.100.141 - 2164     2%
18 ext 203.0.113.29 - 443        1%   ext 203.0.113.26 - 443        2%   int 198.51.100.141 - 38714    2%
19 ext 203.0.113.117 - 443       1%   ext 203.0.113.125 - 443       2%   int 198.51.100.141 - 1932     2%
20 ext 203.0.113.16 - 1935       1%   int 198.51.100.141 - 33778    1%   int 198.51.100.141 - 38158    2%
21 ext 203.0.113.25 - 443        1%   ext 203.0.113.87 - 443        1%   int 198.51.100.141 - 38712    2%
22 ext 203.0.113.115 - 443       1%   ext 203.0.113.87 - 443        1%   int 198.51.100.141 - 2120     2%
23 int 198.51.100.141 - 36124    1%   int 198.51.100.141 - 46448    1%   int 198.51.100.141 - 2159     2%
24 ext 203.0.113.194 - 80        1%   ext 198.51.100.155 - 443      1%   int 198.51.100.141 - 2160     2%
```

Each column lists the top 50 most active endpoints for a single day, starting from the current day, up to the last 500 days. Use the Left / Right arrow keys to move forward / backward in time, or hit Enter and choose menu option *Select Date*. Use the Up / Down arrow keys (or PageUp / PageDown) to access the full 50 endpoints or to move to a different endpoint type. The current day list is updated every 15 minutes.

Daily View

To drill down on a single endpoint and view detailed analytics over a 24 hour period, highlight an endpoint in the Active Endpoint screen, hit Enter and choose menu option *Day*:

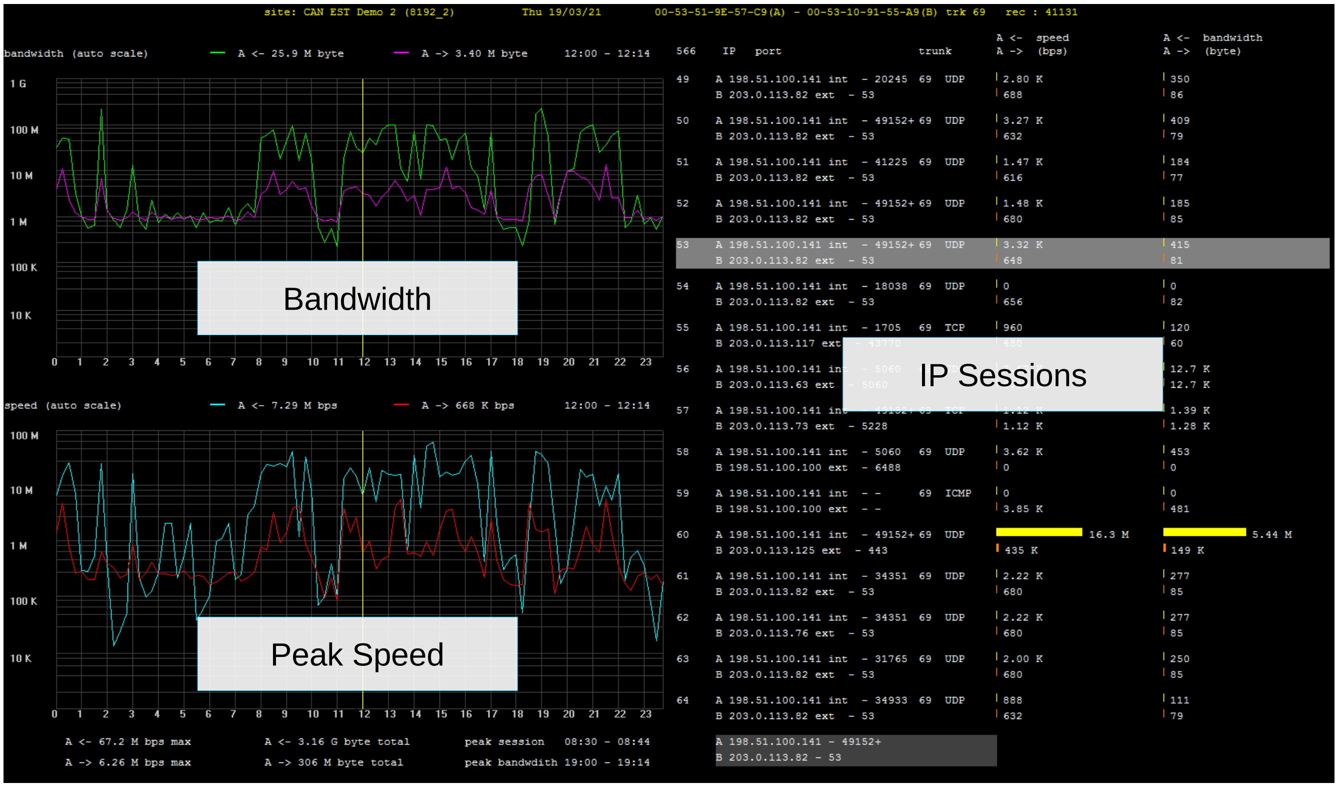


```
                              site: Fax SIP - Primary (8193_5)     RightFax SIP  198.51.100.195 5060   trk 9(A)       Thu 18/08/09

         setup time          trunk / dir        int / ext number                   call state

1        12:00:11            0   in             1660808822    1884006262 name masked   ans release              length   00:00:41
2        12:00:13            0   in             1660468200    1824202680 name masked   ans release              length   00:00:43
3        12:00:28            0   in             1660468200    1844400488 name masked   ans release              length   00:01:10
4        12:00:35            0   in             1662460842    1840602460 name masked   ans release              length   00:00:48
5        12:00:34            0   out            1662846082 name masked   18820024444   nAns fail                486   Client Error   Busy here / Q931 cc 17 User busy
6        12:00:53            0   in             1662460842    1866204862 name masked   ans release              length   00:01:36
7        12:00:50            0   out            1662846082 name masked   18820024444   nAns fail                486   Client Error   Busy here / Q931 cc 17 User busy
8        12:01:02            0   in             1660468200    1264046662 name masked   ans release              length   00:02:01
9        12:01:04            0   in             1660808822    1826446464 name masked   ans release              length   00:00:58
10       12:01:06            0   in             1660468200    1604826600 name masked   ans release              length   00:01:47
11       12:01:11            0   in             1668082486    1604040006 name masked   ans release              length   00:00:39
12       12:01:13            0   in             1662460842    102028240 name masked    ans release              length   00:02:32
13       12:01:20            0   out            1662846082 name masked   18820024444   nAns fail                486   Client Error   Busy here / Q931 cc 17 User busy
14       12:01:26            0   in             1660808822    1840042284 name masked   ans release              length   00:00:44
15       12:01:39            0   in             1660468200    1664684664 name masked   ans release              length   00:00:47
16       12:01:58            0   in             1660808806    1080484848 name masked   ans release              length   00:00:44
```

The format of the daily view depends on endpoint type. The example above is for SIP trunk endpoints. For all endpoint types, use the Left / Right arrow keys to highlight a different 15-minute interval of the day, hit Enter to access a menu of further options, and hit Esc to return to the Active Endpoint screen.

All endpoint types have a menu option *Select Date* to move to a new day without returning to the Active Endpoint screen.

The example below illustrates the format of the daily view for IP endpoints (IP – Port, IP, and IP Trunk). EtherType endpoints do not have a daily view.



```
                         site: CAN EST Demo 2 (8192_2)        Thu 19/03/21        00-53-51-9E-57-C9(A) - 00-53-10-91-55-A9(B) trk 69   rec : 41131

                                                                                                                A <-  speed               A <-  bandwidth
bandwidth (auto scale)     — A <- 25.9 M byte     — A -> 3.40 M byte    12:00 - 12:14   566   IP  port                  trunk   A ->  (bps)               A ->  (byte)

                                                                                        49   A 198.51.100.141 int  - 20245  69  UDP  2.80 K                    350
                                                                                             B 203.0.113.82 ext  - 53                688                       86

                                                                                        50   A 198.51.100.141 int  - 49152+ 69  UDP  3.27 K                    409
                                                                                             B 203.0.113.82 ext  - 53                632                       79

                                                                                        51   A 198.51.100.141 int  - 41225  69  UDP  1.47 K                    184
                                                                                             B 203.0.113.82 ext  - 53                616                       77

                                                                                        52   A 198.51.100.141 int  - 49152+ 69  UDP  1.48 K                    185
                                                                                             B 203.0.113.82 ext  - 53                680                       85

                                                                                        53   A 198.51.100.141 int  - 49152+ 69  UDP  3.32 K                    415
                                                                                             B 203.0.113.82 ext  - 53                648                       81

                                                                                        54   A 198.51.100.141 int  - 18038  69  UDP  0                         0
                                                                                             B 203.0.113.82 ext  - 53                656                       82

                                                                                        55   A 198.51.100.141 int  - 1705   69  TCP  960                       120
                                                                                             B 203.0.113.117 ext  - 43770            480                       60

                                                                                        56   A 198.51.100.141 int  - 5060                                      12.7 K
speed (auto scale)         — A <- 7.29 M bps      — A -> 668 K bps      12:00 - 12:14        B 203.0.113.63 ext  - 5060                                        12.7 K

                                                                                        57   A 198.51.100.141 int  - 49152+ 69  TCP  1.12 K                    1.39 K
                                                                                             B 203.0.113.73 ext  - 5228              1.12 K                    1.28 K

                                                                                        58   A 198.51.100.141 int  - 5060   69  UDP  3.62 K                    453
                                                                                             B 198.51.100.100 ext  - 6488            0                         0

                                                                                        59   A 198.51.100.141 int  - -      69  ICMP 0                         0
                                                                                             B 198.51.100.100 ext  - -               3.85 K                    481

                                                                                        60   A 198.51.100.141 int  - 49152+ 69  UDP  ████████ 16.3 M           ████████ 5.44 M
                                                                                             B 203.0.113.125 ext  - 443              435 K                     149 K

                                                                                        61   A 198.51.100.141 int  - 34351  69  UDP  2.22 K                    277
                                                                                             B 203.0.113.82 ext  - 53                680                       85

                                                                                        62   A 198.51.100.141 int  - 34351  69  UDP  2.22 K                    277
                                                                                             B 203.0.113.76 ext  - 53                680                       85

                                                                                        63   A 198.51.100.141 int  - 31765  69  UDP  2.00 K                    250
                                                                                             B 203.0.113.82 ext  - 53                680                       85

                                                                                        64   A 198.51.100.141 int  - 34933  69  UDP  888                       111
                                                                                             B 203.0.113.82 ext  - 53                632                       79

    A <- 67.2 M bps max     A <- 3.16 G byte total    peak session    08:30 - 08:44          A 198.51.100.141 - 49152+
    A -> 6.26 M bps max     A -> 306 M byte total     peak bandwdith 19:00 - 19:14           B 203.0.113.82 - 53
```

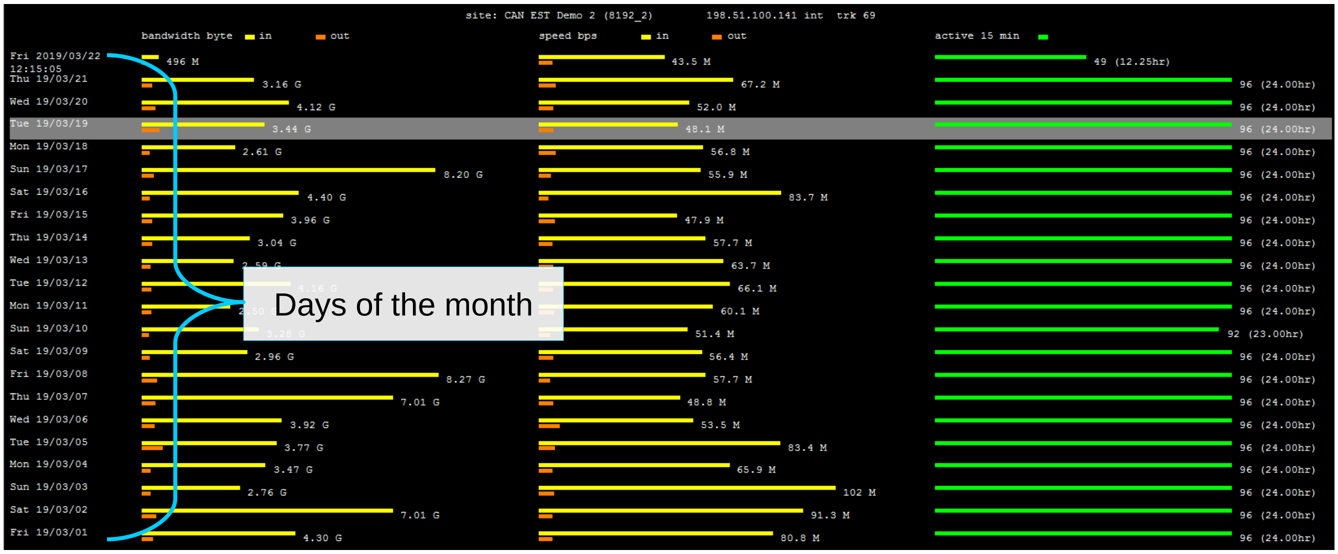
Bandwidth

IP Sessions

Peak Speed

Monthly View

To view analytics for a network endpoint over a month period, highlight an endpoint in the Active Endpoint screen, hit Enter and choose menu option *Month*:



```
                                          site: CAN EST Demo 2 (8192_2)       198.51.100.141 int  trk 69

                bandwidth byte  ▬ in   ▬ out             speed bps   ▬ in   ▬ out             active 15 min  ▬

Fri 2019/03/22                  496 M                                43.5 M                   49 (12.25hr)
12:15:05
Thu 19/03/21                    3.16 G                               67.2 M                   96 (24.00hr)
Wed 19/03/20                    4.12 G                               52.0 M                   96 (24.00hr)
Tue 19/03/19                    3.44 G                               48.1 M                   96 (24.00hr)
Mon 19/03/18                    2.61 G                               56.8 M                   96 (24.00hr)
Sun 19/03/17                    8.20 G                               55.9 M                   96 (24.00hr)
Sat 19/03/16                    4.40 G                               83.7 M                   96 (24.00hr)
Fri 19/03/15                    3.96 G                               47.9 M                   96 (24.00hr)
Thu 19/03/14                    3.04 G                               57.7 M                   96 (24.00hr)
Wed 19/03/13                    2.59 G                               63.7 M                   96 (24.00hr)
Tue 19/03/12                    4.16 G                               66.1 M                   96 (24.00hr)
Mon 19/03/11                    2.50 G                               60.1 M                   96 (24.00hr)
Sun 19/03/10                    3.28 G                               51.4 M                   92 (23.00hr)
Sat 19/03/09                    2.96 G                               56.4 M                   96 (24.00hr)
Fri 19/03/08                    8.27 G                               57.7 M                   96 (24.00hr)
Thu 19/03/07                    7.01 G                               48.8 M                   96 (24.00hr)
Wed 19/03/06                    3.92 G                               53.5 M                   96 (24.00hr)
Tue 19/03/05                    3.77 G                               83.4 M                   96 (24.00hr)
Mon 19/03/04                    3.47 G                               65.9 M                   96 (24.00hr)
Sun 19/03/03                    2.76 G                               102 M                    96 (24.00hr)
Sat 19/03/02                    7.01 G                               91.3 M                   96 (24.00hr)
Fri 19/03/01                    4.30 G                               80.8 M                   96 (24.00hr)
```

Days of the month

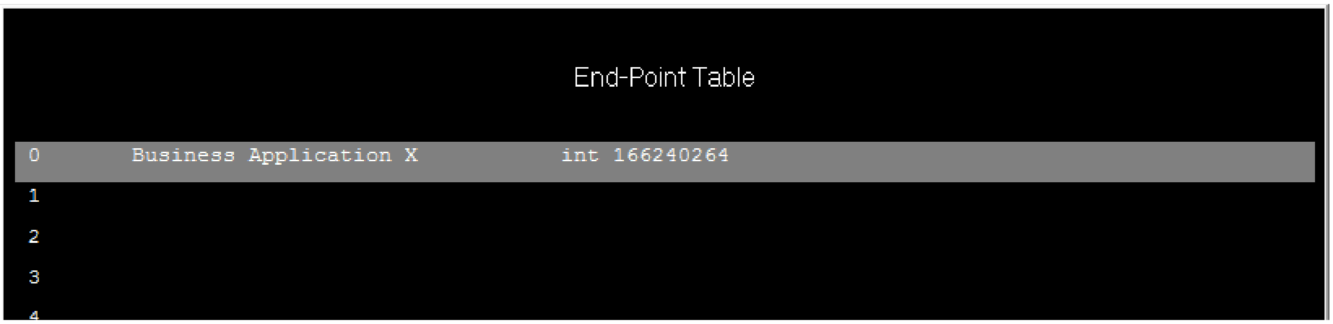
The columns appearing in Monthly View depend on endpoint type. The example above is for IP endpoints. For all endpoint types, use the Up / Down arrow keys to highlight a different day of the month, hit Enter to access a menu of further options, and hit Esc to return to the Active Endpoint screen.

All endpoint types have a menu option *Day* to enter Daily View for the highlighted day, and a menu option *Select Month* to move to any month in the last 16 months.

Search Endpoint

Search Endpoint allows you to quickly access analytics for an endpoint without scanning through the Active Endpoint screen. Furthermore, some endpoints may not appear in the Active Endpoint screen because they do not have enough traffic to fall in the top 50 on any day. Such endpoints are only accessible through the Search Endpoint feature.

Highlight an IP-Meter from the main screen, hit Enter and choose menu option *Search Endpoint*:



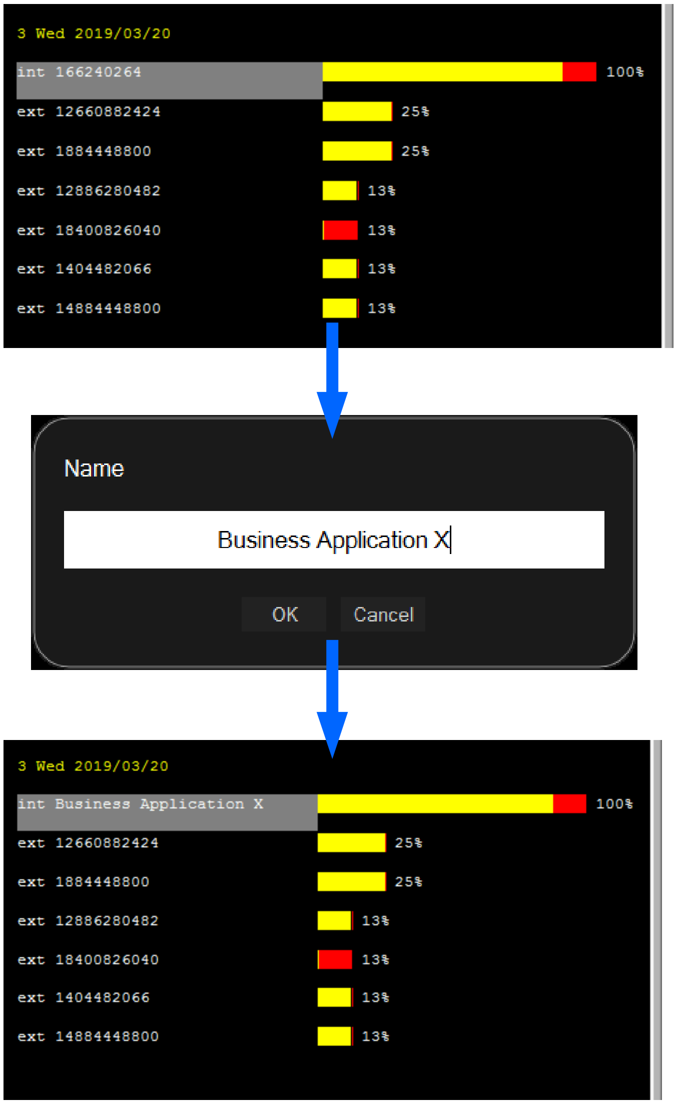
```
                              End-Point Table

0       Business Application X          int 166240264
1
2
3
4
```

The **Endpoint Table** is a place to store endpoints for quick access and to assign meaningful names. To add an endpoint, highlight the first empty row, hit Enter and choose a type (IP, IP – Port, IP – IP, or SIP Number). In the above example, a single SIP Number endpoint has been added called “Business Application X”.

To access analytics for an endpoint, highlight the endpoint in the Endpoint Table, hit Enter and choose menu option *Traffic*.

Add to Endpoint Table from Active Endpoint Screen

In addition to manually editing the Endpoint table, you can add endpoints directly from the Active Endpoint screen:



```
3 Wed 2019/03/20
int 166240264          100%
ext 12660882424        25%
ext 1884448800         25%
ext 12886280482        13%
ext 18400826040        13%
ext 1404482066         13%
ext 14884448800        13%
```

```
3 Wed 2019/03/20
int Business Application X   100%
ext 12660882424              25%
ext 1884448800               25%
ext 12886280482              13%
ext 18400826040              13%
ext 1404482066               13%
ext 14884448800              13%
```

1. Highlight an endpoint, hit Enter and choose menu option *Add to Endpoint Table*.

2. Enter a meaningful name for the endpoint.

3. Endpoint name is updated in the Active Endpoint screen, and any other screen where the endpoint is referenced.

SIP Group / Route Analytics

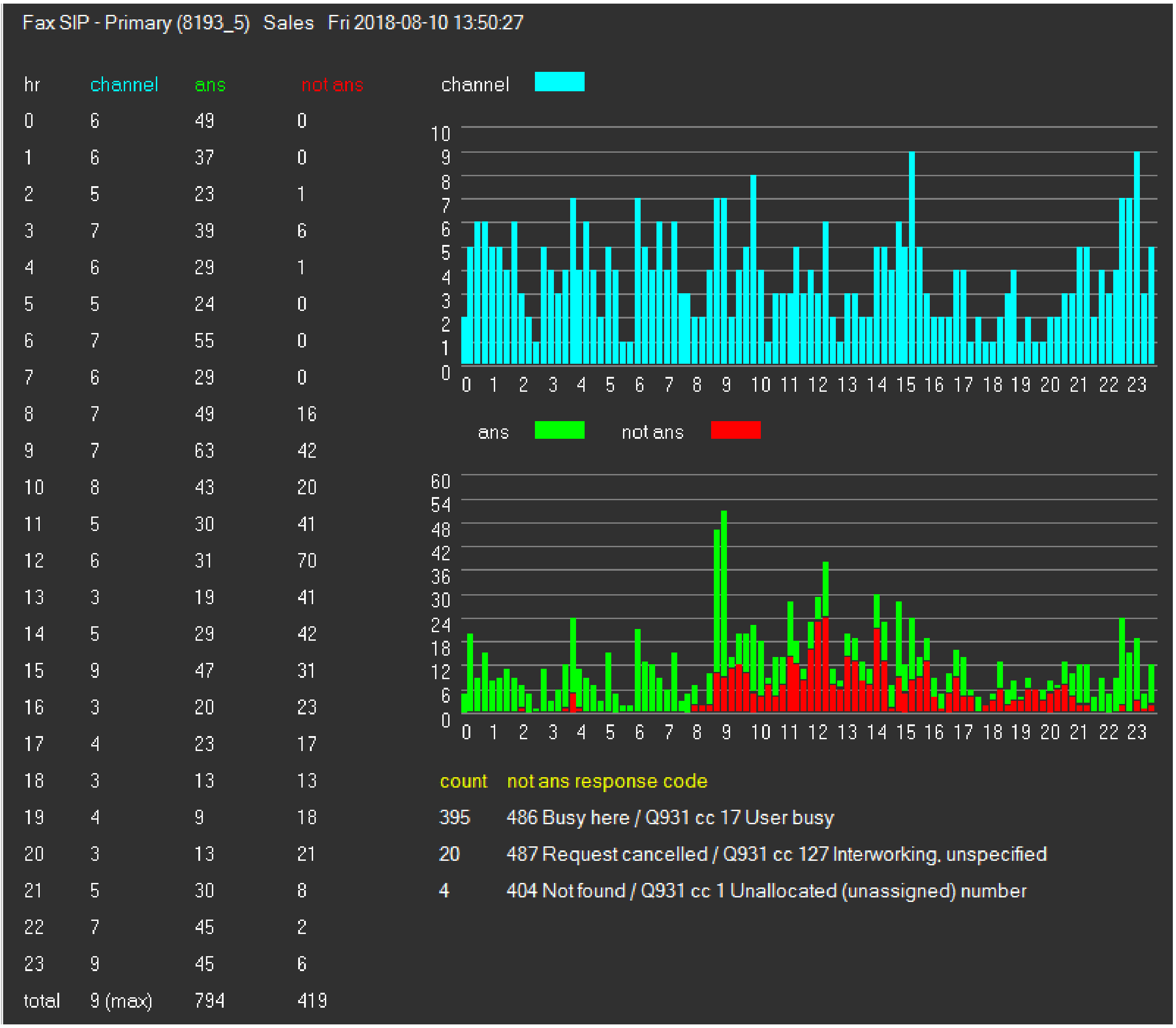
The IP-Meter will automatically compile analytics for each SIP Number endpoint. In addition, the user can define *SIP groups* to track combinations of phone numbers, such as a routes, ACD queues, or other important business applications (see SIP Group Table for details).

To view analytics for a SIP Group, highlight then IP-Meter on the main screen, hit Enter and choose menu option *SIP Group*. Then highlight the SIP group you wish to analyze, hit Enter and choose menu option *Analytics*. The Monthly View and Daily View for SIP Groups share the same format as SIP trunks.

SIP Group / Route Daily Summary

The Daily View for SIP groups has one additional feature that allows you to view multiple days or multiple groups simultaneously.

While in Daily View, hit Enter and choose menu option *Summary*. This will pop out a new window which will remain visible if you exit Daily View to select another group or another day.



Fax SIP - Primary (8193_5) Sales Fri 2018-08-10 13:50:27

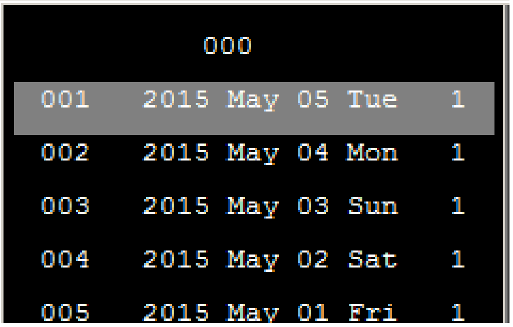
hr	channel	ans	not ans
0	6	49	0
1	6	37	0
2	5	23	1
3	7	39	6
4	6	29	1
5	5	24	0
6	7	55	0
7	6	29	0
8	7	49	16
9	7	63	42
10	8	43	20
11	5	30	41
12	6	31	70
13	3	19	41
14	5	29	42
15	9	47	31
16	3	20	23
17	4	23	17
18	3	13	13
19	4	9	18
20	3	13	21
21	5	30	8
22	7	45	2
23	9	45	6
total	9 (max)	794	419

count	not ans response code
395	486 Busy here / Q931 cc 17 User busy
20	487 Request cancelled / Q931 cc 127 Interworking, unspecified
4	404 Not found / Q931 cc 1 Unallocated (unassigned) number

Multiple SIP group summary windows can be open and arranged on your screen, effectively creating a custom dashboard. Summaries that show the current date will update every 15 minutes. To close a summary, select the window and hit *Esc* key.

Generating Reports

All data for each site can be exported in CSV format, and summary reports can be generated in PDF format. Highlight an IP-Meter from the main screen, hit Enter and choose menu option *Report*:

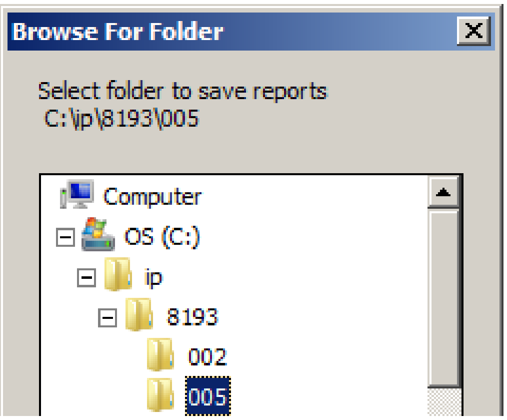


```
              000
001    2015 May 05 Tue    1
002    2015 May 04 Mon    1
003    2015 May 03 Sun    1
004    2015 May 02 Sat    1
005    2015 May 01 Fri    1
```

Select which date to export.

A *1* appears beside each date that has data available.

A *0* indicates that no data is available for that date.



Select folder to save reports
C:\ip\8193\005

Browse for a folder to save report files.

Once you hit OK and the report process completes, Windows explorer will open to display the files in the folder that you selected.

Up to 7 report files created. Each file name is prefixed by date and IP-Meter number. The format of the date prefix is YYMMDD.

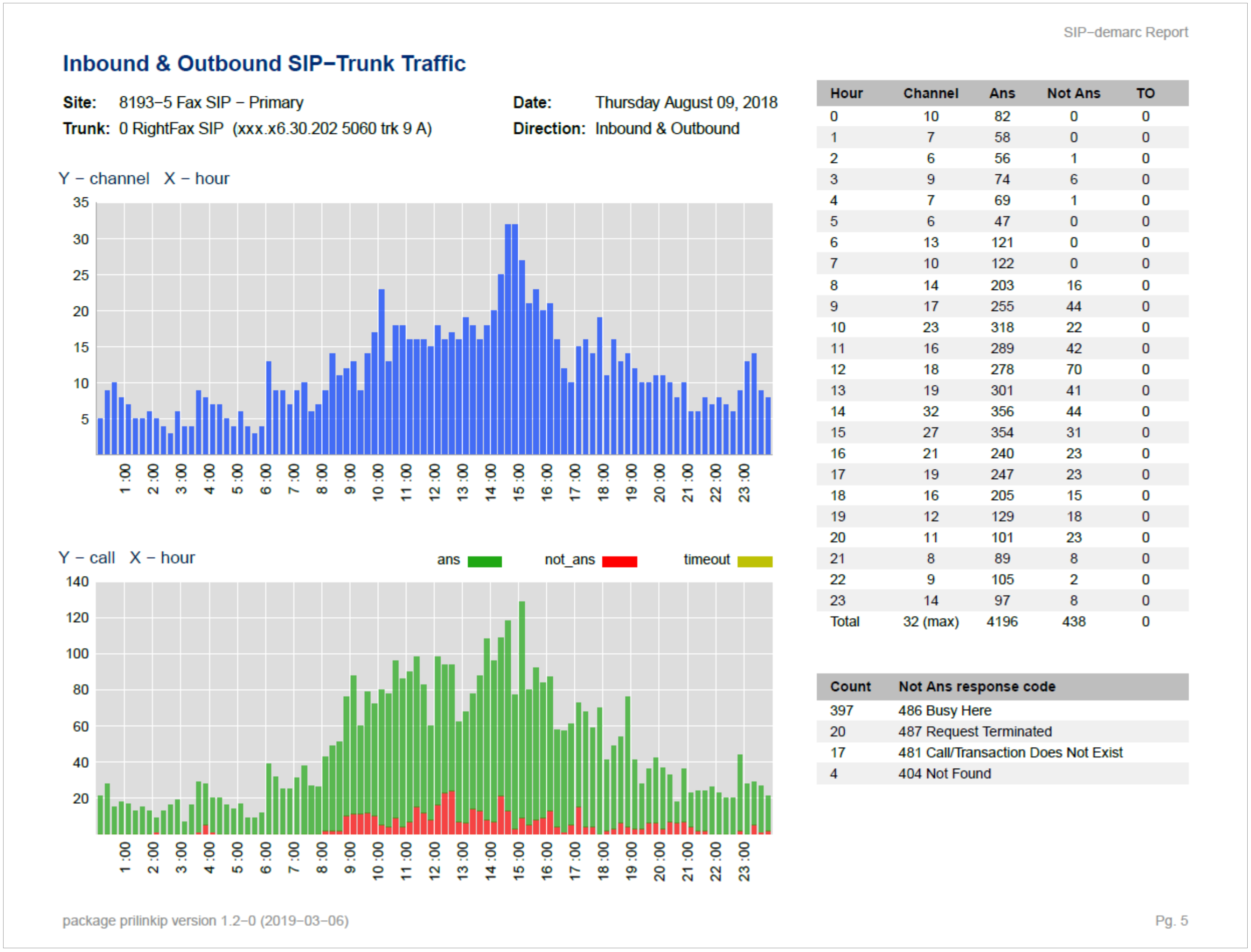
e.g. “`170225-8190-3 sip-report.pdf`” for February 25th 2017, IP-Meter number 8190-3.

The files created are summarized below:

`sip-cdr.csv`	Call Detail Records for each sip call, including MOS information.
`sip-trunk-records.csv`	15-minute traffic statistics for each SIP trunk.
`sip-group-records.csv`	15-minute traffic statistics for each SIP group / route.
`ip-cdr.csv`	Connection Detail Records for each IP session.
`ip-trunk-records.csv`	15-minute traffic statistics for each IP Trunk.
`sip-report.pdf`	SIP summary PDF report.
`ip-report.pdf`	IP summary PDF report.

The SIP summary PDF report includes inbound / outbound summary, SIP trunk traffic summary and SIP group traffic summary.

Below is a sample page showing 15-minute call volume and call blockage summary for SIP trunk #0:



SIP–demarc Report

Inbound & Outbound SIP–Trunk Traffic

Site: 8193–5 Fax SIP – Primary
Trunk: 0 RightFax SIP (xxx.x6.30.202 5060 trk 9 A)
Date: Thursday August 09, 2018
Direction: Inbound & Outbound

Hour	Channel	Ans	Not Ans	TO
0	10	82	0	0
1	7	58	0	0
2	6	56	1	0
3	9	74	6	0
4	7	69	1	0
5	6	47	0	0
6	13	121	0	0
7	10	122	0	0
8	14	203	16	0
9	17	255	44	0
10	23	318	22	0
11	16	289	42	0
12	18	278	70	0
13	19	301	41	0
14	32	356	44	0
15	27	354	31	0
16	21	240	23	0
17	19	247	23	0
18	16	205	15	0
19	12	129	18	0
20	11	101	23	0
21	8	89	8	0
22	9	105	2	0
23	14	97	8	0
Total	32 (max)	4196	438	0

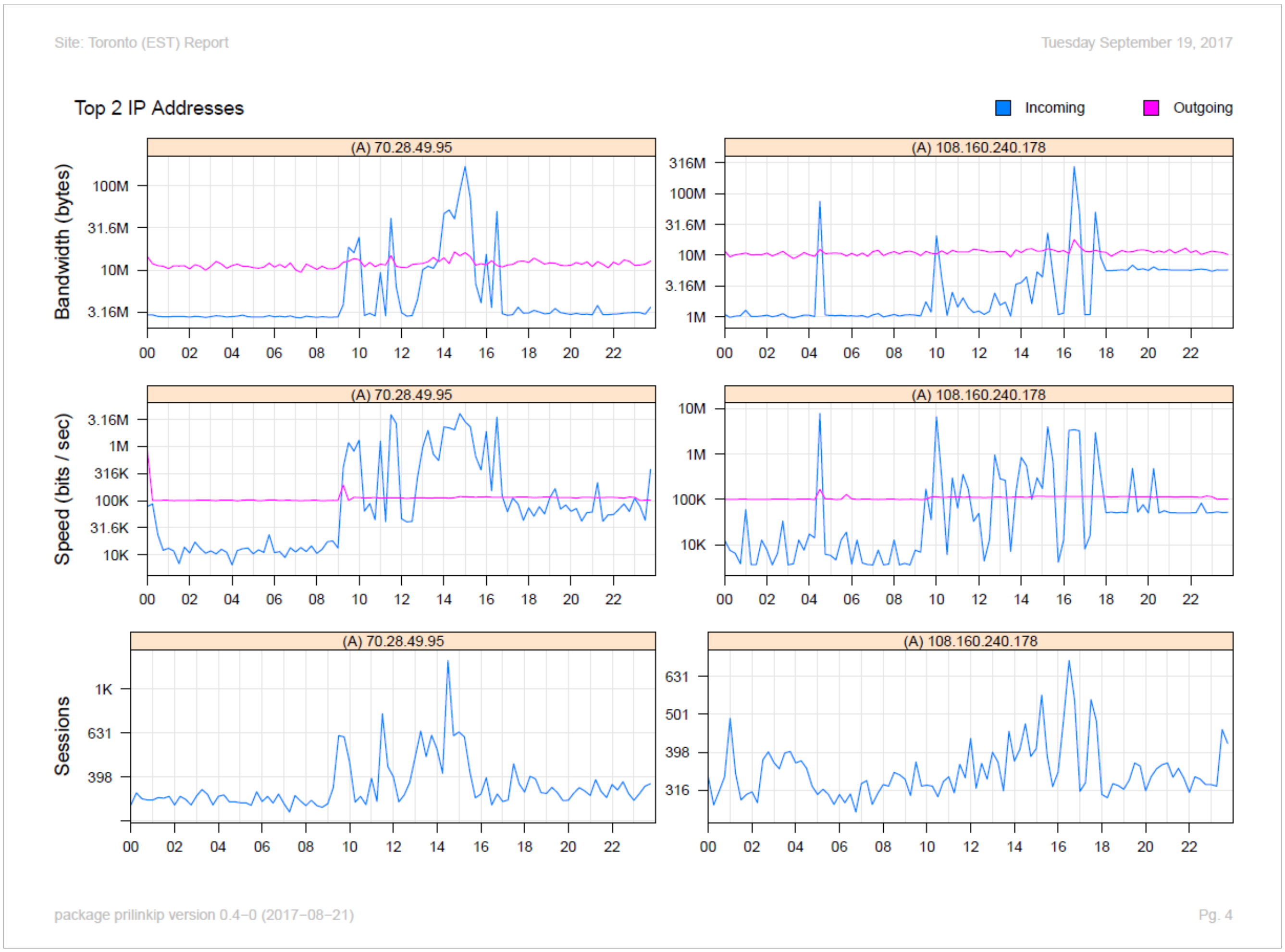
Count	Not Ans response code
397	486 Busy Here
20	487 Request Terminated
17	481 Call/Transaction Does Not Exist
4	404 Not Found

package prilinkip version 1.2–0 (2019–03–06)

Pg. 5

The IP summary PDF report tabulates the top 30 IP endpoints (IP – Port, IP, & IP trunk), and includes charts for the top 2 endpoints in each category.

Below is a sample page showing 15-min bandwidth and speed for the top 2 IP address endpoints:



Site: Toronto (EST) Report

Tuesday September 19, 2017

Top 2 IP Addresses

package prilinkip version 0.4–0 (2017–08–21)

Pg. 4

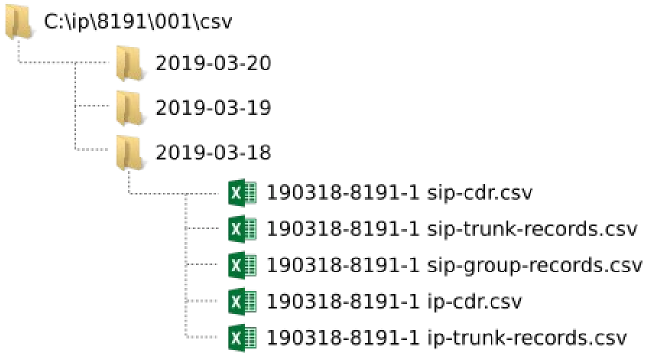
Automatic Daily Reports

If the PrilinkNM application is running and connected to an IP-Meter, it will automatically generate all 7 report files at the end of each day, as well as every 15 minutes for the current day. The files are deposited in the IP-Meter site directory.

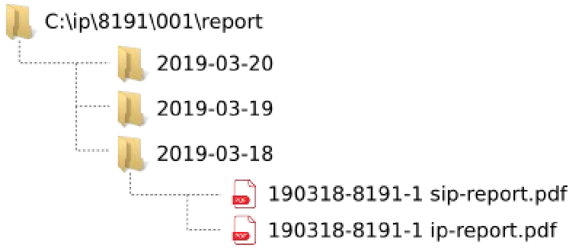
Site Directory

Data for each IP-Meter is stored locally on your PC / Server in the directory `C:\ip\`*xxxx*`\00`*y*, where *xxxx*-*y* is the IP-Meter site number. E.g., the site directory for IP-Meter 8191-1 is `C:\ip\8191\001`. A complete backup of site data can be achieved simply by backup up this directory.

Within the site directory, daily report files are deposited in the *csv* and *report* sub-directories as shown below:



C:\ip\8191\001\csv
- 2019-03-20
- 2019-03-19
- 2019-03-18
  - 190318-8191-1 sip-cdr.csv
  - 190318-8191-1 sip-trunk-records.csv
  - 190318-8191-1 sip-group-records.csv
  - 190318-8191-1 ip-cdr.csv
  - 190318-8191-1 ip-trunk-records.csv



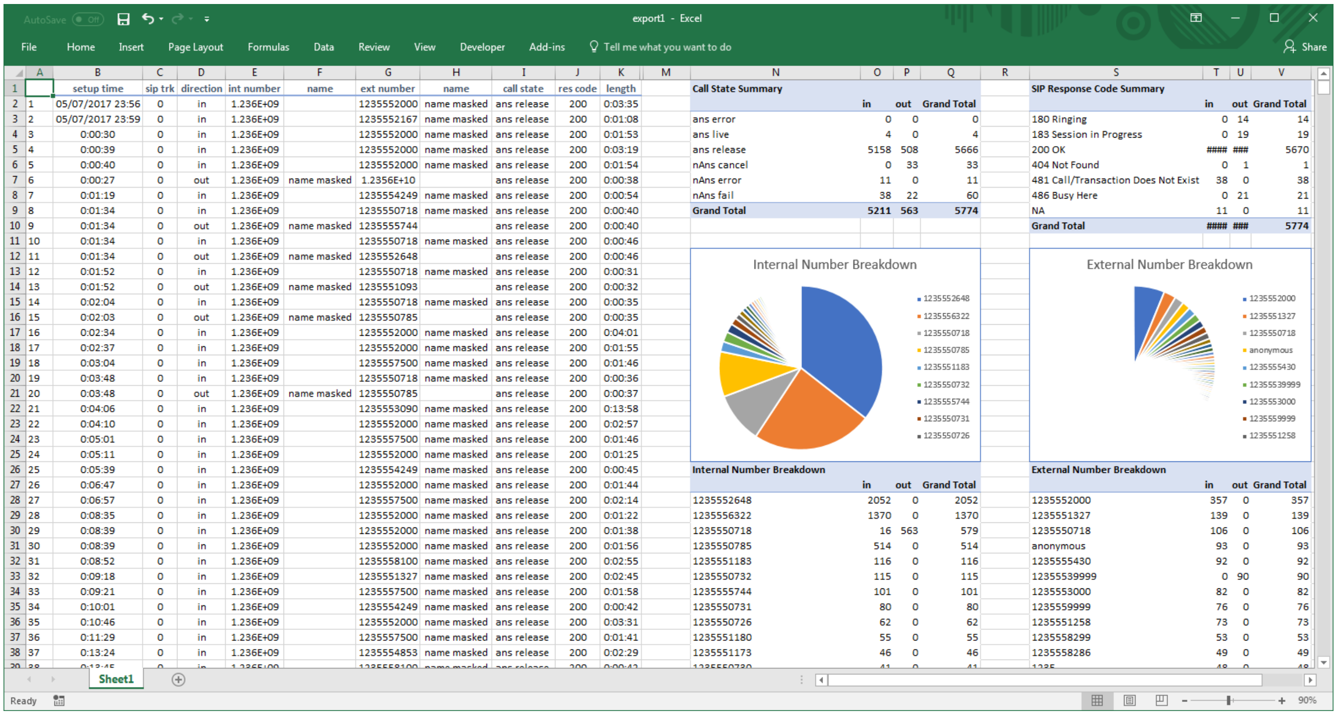
C:\ip\8191\001\report
- 2019-03-20
- 2019-03-19
- 2019-03-18
  - 190318-8191-1 sip-report.pdf
  - 190318-8191-1 ip-report.pdf

Export data to Microsoft Excel

Many screens in the PrilinkNM application include the menu option *Export*. This option exports screen data into a CSV file, which is then normally opened using the default application for CSV files on your system.

However, before opening the CSV file, the application first searches for an MS Excel template under `C:\ip\export.xltm`, and attempts to run this template if it exists. If you wish to make use of this template, simply download `export.xltm` from http://prilink.com/downloads/ and save the file under your `C:\ip` directory. The use of macros must be permitted for the template to function.

Below is an example from created from SIP trunk Daily View by choosing menu option *Export CDR*.



	setup time	sip trk	direction	int number	name	ext number	name	call state	res code	length
1	05/07/2017 23:56	0	in	1.236E+09		1235552000	name masked	ans release	200	0:03:35
2	05/07/2017 23:59	0	in	1.236E+09		1235552167	name masked	ans release	200	0:01:08
3	0:00:30	0	in	1.236E+09		1235552000	name masked	ans release	200	0:01:53
4	0:00:39	0	in	1.236E+09		1235552000	name masked	ans release	200	0:03:19
5	0:00:40	0	in	1.236E+09		1235552000	name masked	ans release	200	0:01:54
6	0:00:27	0	out	1.236E+09	name masked	1.2356E+10		ans release	200	0:00:38
7	0:01:19	0	in	1.236E+09		1235554249	name masked	ans release	200	0:00:54
8	0:01:34	0	in	1.236E+09		1235550718	name masked	ans release	200	0:00:40
9	0:01:34	0	out	1.236E+09	name masked	1235555744		ans release	200	0:00:40
10	0:01:34	0	in	1.236E+09		1235550718	name masked	ans release	200	0:00:46
11	0:01:34	0	out	1.236E+09	name masked	1235552648		ans release	200	0:00:46
12	0:01:52	0	in	1.236E+09		1235550718	name masked	ans release	200	0:00:31
13	0:01:52	0	out	1.236E+09	name masked	1235551093		ans release	200	0:00:32
14	0:02:04	0	in	1.236E+09		1235550718	name masked	ans release	200	0:00:35
15	0:02:03	0	out	1.236E+09	name masked	1235550785		ans release	200	0:00:35
16	0:02:34	0	in	1.236E+09		1235552000	name masked	ans release	200	0:04:01
17	0:02:37	0	in	1.236E+09		1235552000	name masked	ans release	200	0:01:55
18	0:03:04	0	in	1.236E+09		1235557500	name masked	ans release	200	0:01:46
19	0:03:48	0	in	1.236E+09		1235550718	name masked	ans release	200	0:00:36
20	0:03:48	0	out	1.236E+09	name masked	1235550785		ans release	200	0:00:37
21	0:04:06	0	in	1.236E+09		1235553090	name masked	ans release	200	0:13:58
22	0:04:10	0	in	1.236E+09		1235552000	name masked	ans release	200	0:02:57
23	0:05:01	0	in	1.236E+09		1235557500	name masked	ans release	200	0:01:46
24	0:05:11	0	in	1.236E+09		1235552000	name masked	ans release	200	0:01:25
25	0:05:39	0	in	1.236E+09		1235554249	name masked	ans release	200	0:00:45
26	0:06:47	0	in	1.236E+09		1235552000	name masked	ans release	200	0:01:44
27	0:06:57	0	in	1.236E+09		1235557500	name masked	ans release	200	0:02:14
28	0:08:35	0	in	1.236E+09		1235552000	name masked	ans release	200	0:01:22
29	0:08:39	0	in	1.236E+09		1235552000	name masked	ans release	200	0:01:38
30	0:08:39	0	in	1.236E+09		1235552000	name masked	ans release	200	0:01:56
31	0:08:52	0	in	1.236E+09		1235558100	name masked	ans release	200	0:02:55
32	0:09:18	0	in	1.236E+09		1235551327	name masked	ans release	200	0:02:45
33	0:09:21	0	in	1.236E+09		1235557500	name masked	ans release	200	0:01:58
34	0:10:01	0	in	1.236E+09		1235554249	name masked	ans release	200	0:00:42
35	0:10:46	0	in	1.236E+09		1235552000	name masked	ans release	200	0:03:31
36	0:11:29	0	in	1.236E+09		1235557500	name masked	ans release	200	0:01:41
37	0:13:24	0	in	1.236E+09		1235554853	name masked	ans release	200	0:02:29

Call State Summary

	in	out	Grand Total
ans error	0	0	0
ans live	4	0	4
ans release	5158	508	5666
nAns cancel	0	33	33
nAns error	11	0	11
nAns fail	38	22	60
Grand Total	**5211**	**563**	**5774**

SIP Response Code Summary

	in	out	Grand Total
180 Ringing	0	14	14
183 Session in Progress	0	19	19
200 OK	####	###	5670
404 Not Found	0	1	1
481 Call/Transaction Does Not Exist	38	0	38
486 Busy Here	0	21	21
NA	11	0	11
Grand Total	**####**	**###**	**5774**

Internal Number Breakdown

	in	out	Grand Total
1235552648	2052	0	2052
1235556322	1370	0	1370
1235550718	16	563	579
1235550785	514	0	514
1235551183	116	0	116
1235550732	115	0	115
1235555744	101	0	101
1235550731	80	0	80
1235550726	62	0	62
1235551180	55	0	55
1235551173	46	0	46

External Number Breakdown

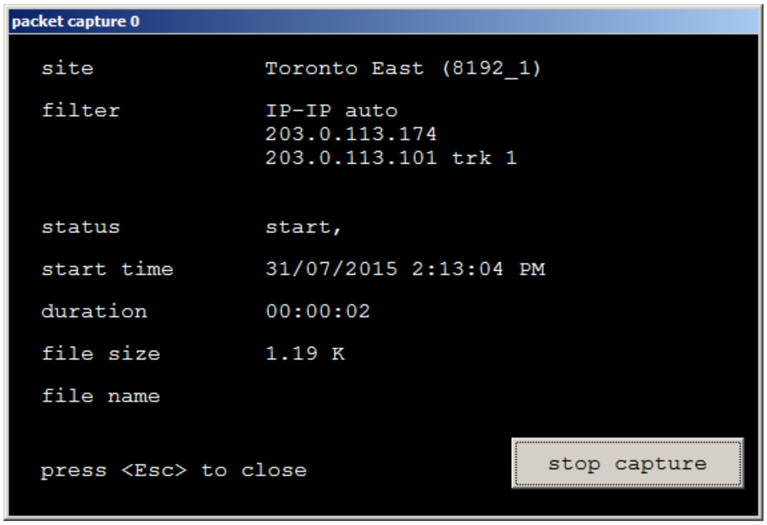
	in	out	Grand Total
1235552000	357	0	357
1235551327	139	0	139
1235550718	106	0	106
anonymous	93	0	93
1235555430	92	0	92
12355539999	0	90	90
1235553000	82	0	82
1235559999	76	0	76
1235551258	73	0	73
1235558299	53	0	53
1235558286	49	0	49

Troubleshooting with Deep Packet Inspection

Analyzing raw network packets is sometimes necessary to troubleshoot problems and gain insight into application operation. All of the network endpoints that are automatically scanned by Prilink can be used as filters for packet capture, alleviating the need to use complex filter syntax. Capture files are saved to the user's PC in Wireshark-compatible format for further investigation.

There are three ways to initiate packet capture for a particular network endpoint:

- Highlight an endpoint in the Active Endpoint screen, hit Enter and choose menu option *Capture Packet*.
- Highlight an endpoint in the Endpoint Table, hit Enter and choose menu option *Capture Packet*.
- Highlight a SIP trunk in the SIP Trunk Table, hit Enter and choose menu option *Capture SIP trunk message* or *Capture SIP number message*. The latter option filters SIP traffic by a specific phone number, useful for testing purposes. Both option capture both SIP signalling and RTP streams for further analysis.



```
packet capture 0

site              Toronto East (8192_1)

filter            IP-IP auto
                  203.0.113.174
                  203.0.113.101 trk 1

status            start,

start time        31/07/2015 2:13:04 PM

duration          00:00:02

file size         1.19 K

file name

press <Esc> to close
```

A Packet Capture window will open.

The *Filter* field indicates the network endpoint used to filter packets.

The *Duration* and *File size* fields are incremented as the capture progresses and more packets are added to the capture file. Capture will continue until a maximum file size is reached or until the user clicks the *Stop Capture* button.

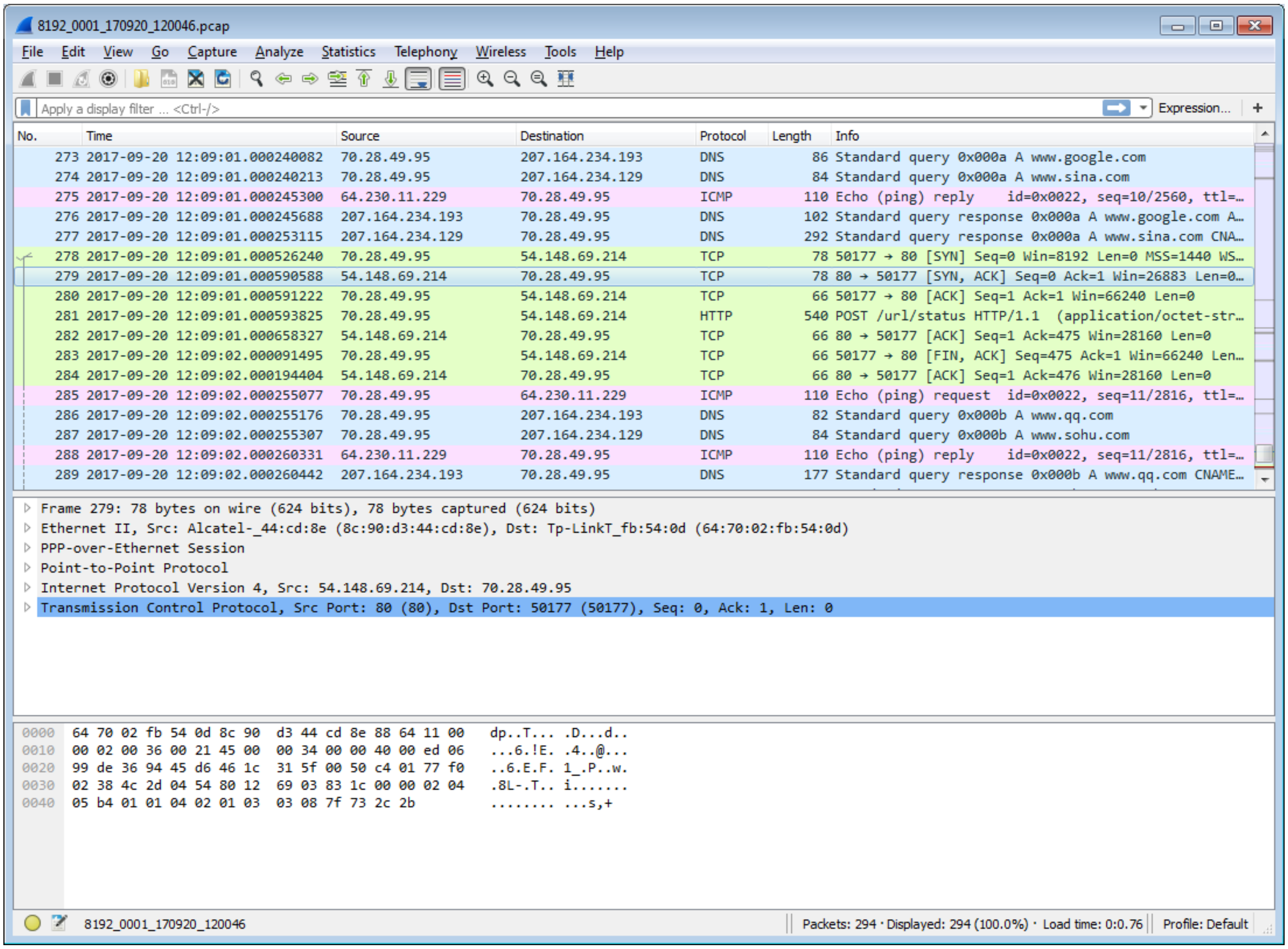
Once complete, the *Status* field will reach “end” and the *File name* field will update to indicate the full path where the capture file is stored. Two files are created in the process:

{site number}_{YYMMDD}_{HHMMSS}.pcap	Raw capture file.
{site number}_{YYMMDD}_{HHMMSS}.txt	Text file containing all metadata from the Packet Capture window (filter, start time, duration, etc).

It is possible to initiate packet capture on multiple sites simultaneously; a separate Packet Capture window will open for each site.

Open Capture File in Wireshark

Once a packet capture is completed, the *stop capture* button will be renamed to *Open File*. Clicking the *Open File* button will attempt to use the default application for opening `.pcap` files on your system. If you have installed the Wireshark application, the installation process will normally associate `.pcap` files with Wireshark, so that clicking *Open File* will trigger Wireshark.


8192_0001_170920_120046.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
8192_0001_170920_120046
Packets: 294 · Displayed: 294 (100.0%) · Load time: 0:0.76
Profile: Default

```
No.      Time                           Source            Destination       Protocol  Length  Info
     273 2017-09-20 12:09:01.000240082  70.28.49.95       207.164.234.193   DNS           86 Standard query 0x000a A www.google.com
     274 2017-09-20 12:09:01.000240213  70.28.49.95       207.164.234.129   DNS           84 Standard query 0x000a A www.sina.com
     275 2017-09-20 12:09:01.000245300  64.230.11.229     70.28.49.95       ICMP         110 Echo (ping) reply    id=0x0022, seq=10/2560, ttl=…
     276 2017-09-20 12:09:01.000245688  207.164.234.193   70.28.49.95       DNS          102 Standard query response 0x000a A www.google.com A…
     277 2017-09-20 12:09:01.000253115  207.164.234.129   70.28.49.95       DNS          292 Standard query response 0x000a A www.sina.com CNA…
     278 2017-09-20 12:09:01.000526240  70.28.49.95       54.148.69.214     TCP           78 50177 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS…
     279 2017-09-20 12:09:01.000590588  54.148.69.214     70.28.49.95       TCP           78 80 → 50177 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0…
     280 2017-09-20 12:09:01.000591222  70.28.49.95       54.148.69.214     TCP           66 50177 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
     281 2017-09-20 12:09:01.000593825  70.28.49.95       54.148.69.214     HTTP         540 POST /url/status HTTP/1.1  (application/octet-str…
     282 2017-09-20 12:09:01.000658327  54.148.69.214     70.28.49.95       TCP           66 80 → 50177 [ACK] Seq=1 Ack=475 Win=28160 Len=0
     283 2017-09-20 12:09:02.000091495  70.28.49.95       54.148.69.214     TCP           66 50177 → 80 [FIN, ACK] Seq=475 Ack=1 Win=66240 Len…
     284 2017-09-20 12:09:02.000194404  54.148.69.214     70.28.49.95       TCP           66 80 → 50177 [ACK] Seq=1 Ack=476 Win=28160 Len=0
     285 2017-09-20 12:09:02.000255077  70.28.49.95       64.230.11.229     ICMP         110 Echo (ping) request  id=0x0022, seq=11/2816, ttl=…
     286 2017-09-20 12:09:02.000255176  70.28.49.95       207.164.234.193   DNS           82 Standard query 0x000b A www.qq.com
     287 2017-09-20 12:09:02.000255307  70.28.49.95       207.164.234.129   DNS           84 Standard query 0x000b A www.sohu.com
     288 2017-09-20 12:09:02.000260331  64.230.11.229     70.28.49.95       ICMP         110 Echo (ping) reply    id=0x0022, seq=11/2816, ttl=…
     289 2017-09-20 12:09:02.000260442  207.164.234.193   70.28.49.95       DNS          177 Standard query response 0x000b A www.qq.com CNAME…
```

```
▷ Frame 279: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▷ Ethernet II, Src: Alcatel-_44:cd:8e (8c:90:d3:44:cd:8e), Dst: Tp-LinkT_fb:54:0d (64:70:02:fb:54:0d)
▷ PPP-over-Ethernet Session
▷ Point-to-Point Protocol
▷ Internet Protocol Version 4, Src: 54.148.69.214, Dst: 70.28.49.95
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 50177 (50177), Seq: 0, Ack: 1, Len: 0
```

```
0000  64 70 02 fb 54 0d 8c 90  d3 44 cd 8e 88 64 11 00   dp..T... .D...d..
0010  00 02 00 36 00 21 45 00  00 34 00 00 40 00 ed 06   ...6.!E. .4..@...
0020  99 de 36 94 45 d6 46 1c  31 5f 00 50 c4 01 77 f0   ..6.E.F. 1_.P..w.
0030  02 38 4c 2d 04 54 80 12  69 03 83 1c 00 00 02 04   .8L-.T.. i.......
0040  05 b4 01 01 04 02 01 03  03 08 7f 73 2c 2b         ........ ...s,+
```