

**Government of India
Department of Telecommunications
(Data Services Cell)**

No. 820-1/98-LR/Vol(X)(Part-II)

Dated: 16-06-2022

Subject: Compliance of revised IPDR format notified vide DOT letter no 8520-01/98-LR/Vol.(IX) Pt. I dated 16.11.2021.

Kindly refer to the revised IPDR format notified vide DoT letter no.8520-01/98-LR/Vol.(IX) Pt. I dated 16.11.2021 and minutes of meeting dated 12.04.2022.

2. In this regard, only issue raised by operators wrt compliance of said letter of DOT dated 16.11.21 was relating to destination IP, destination port.
3. In order to facilitate ISPs w.r.t. issues in para 2 above, few options have been suggested by C-DOT (copy enclosed) for your information / consideration. In case of any query, you may contact to CDoT: Sh. Pramod Kumar, e-mail id pramods@cdot.in
4. This issues with the approval of competent authority.

Encl:A/A

**(U.C. Meena)
ADG (DS-II)
Tel: 9868131311**

To,

1. All ISPs.

Copy to,

1. PPS to Secretary (T)
2. PPS to Member (T)
3. PPS to DGT, DoT HQ
4. ED CDOT
5. ISPAI

Overview of IPDR (Internet Protocol Detail Record) generation

Prepared by: C-DOT
(V.1.0)

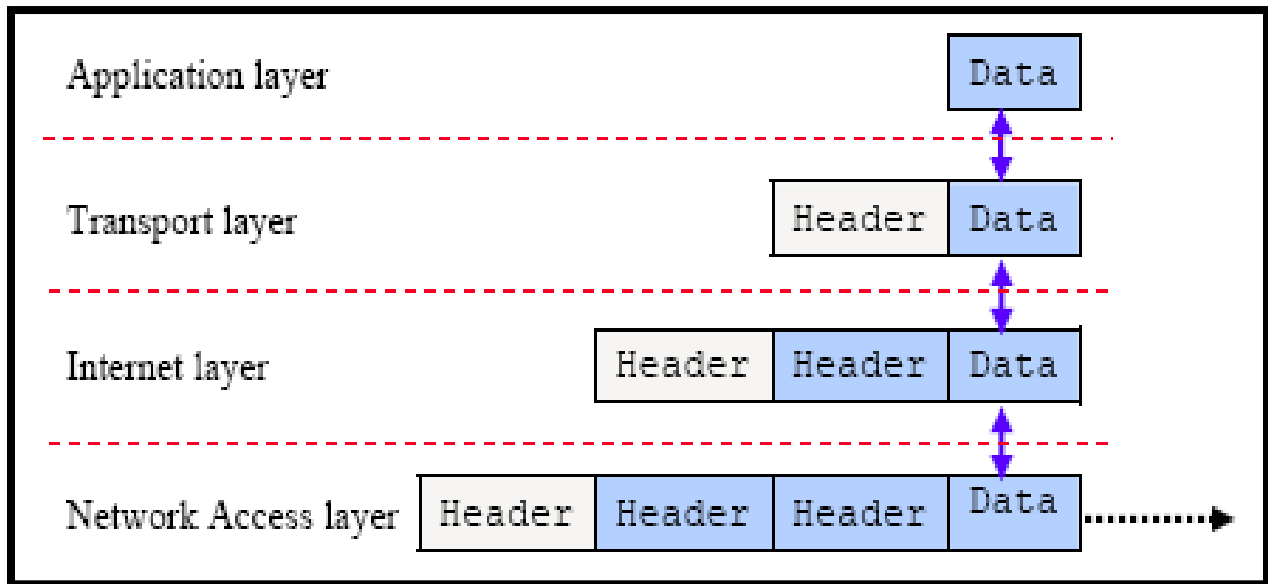
Contents

1. Introduction:	2
2. Mapping of OSI Model with TCP/IP Stack	2
3. IPDR Generation methods:	3
4. C-DOT IPFIX Probe:	3
4.1 IPFIX Flow Collection	4
4.2 Reading Flows: NFCAPD	5
4.3 ProcessingNetFlow / IPFIX Flows:	5
5. Implementation Scenario- 1: ISP sites installed with C-DOT Internet Monitoring System (IMS) .	6
5.1. IPDR Parameters (for IPv4/IPv6) available with IPFIX	6
6. Implementation Scenario2: ISP sites not installed with Internet Monitoring System (IMS)	7
7. Conclusion:	7
Annexure: 1	9
Annexure: 2	11

1. Introduction:

ISP (Internet Service Provider) needs to maintain IPDR (Internet Protocol Detail record) as per mandate requirement of License conditions. IPDR provides information about IP based service usage. DoT had issued guidelines in this regard on 01-10-2013 (Annexure 1) for IPDR parameters to be stored in respect of Internet & GPRS services (like user details, IP address, Static / Dynamic IP address allocation, Source port of Public IP address in case of NATing, IP address allocation start & End time etc.) and modified guidelines were issued on 16.1.11.2021(Annexure-2) in which some additional parameters like Destination IP, Destination ports& Source Port were mentioned (for IPv4 and IPv6) which are to be stored in respect of Wireless / Wireline Internet services.

1.1 Anatomy of a TCP/IP Packet:



2. Mapping of OSI Model with TCP/IP Stack

7	Application layer	FTP, HTTP, HTTPS, IMAP, IRC, NTP, POP3, RTP, SIP, SMTP, SNMP, SSH, SSL, Telnet, DNS,, IMAP/IMAP4, RADIUS, TOR, etc.
4	Transport layer	OSPF, SCTP, TCP, UDP, etc.
3	Network/Internet layer	IPv4, IPv6, ICMP, ARP, IGMP, IPSEC, NAT etc
1, 2	Physical/ Data Link layer	Ethernet, Wireless (WAP, CDPD, 802.11, Wi-Fi), Token ring, FDDI, PPP, ISDN, Frame Relay, ATM, SONET/SDH, xDSL, SLIP etc. RS-232, EIA-422, RS-449, EIA-485 etc.

3. IPDR Generation methods:

Generally used methods for IPDR generation are described below:

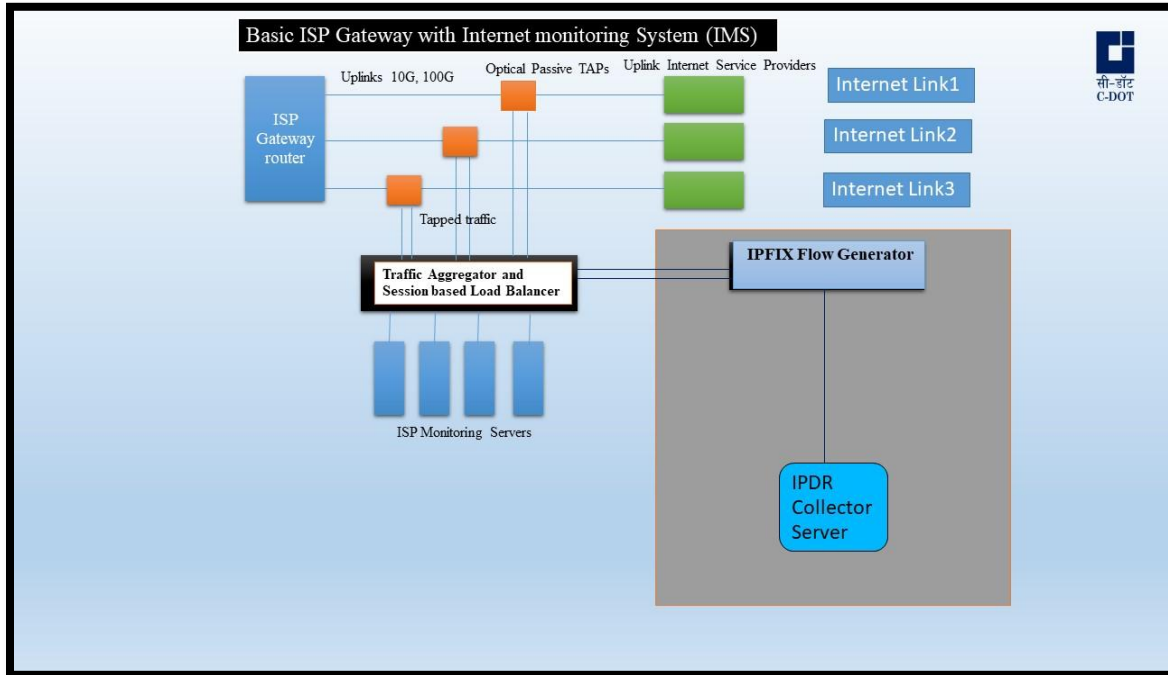
- i) **NetFlow/IPFIX Technology:** NetFlow Network Protocol is used to generate IPDR information (Source IP, Source Port, Destination IP, Destination Port, Flow Start time, Flow end time etc.) on IP network device like Router / Firewall. A NetFlow-enabled device generates metadata at the interface level and sends this information to a flow collector(a separate server), where the flow records are stored to carry out network traffic analytics. NetFlow can be generated on almost all managed network devices. However, Flow generation sampling rate varies from devices to device. Many of the enterprise class network devices have capability to generate flow in 1:1 ratio. If flow generation is on 1:1 ratio, then this method can be used for generating required IPDR logs.
- ii) IPDR information (Source IP, Source Port, Destination IP, Destination Port, Flow Start time, Flow end time etc.) is also available in Syslog generated in Firewall or Integrated Router / Firewall which can be transferred to a separate log server. Logs of network devices thus transferred to log server can be stored at some defined interval. These logs provide the IPDR information. Customized scripts can be used to retrieve required information from logs. So syslog generation method is another method for IPDR generation. This method is also referred to as NATing.
- iii) IPFIX (Internet Protocol Flow Information Export) can also be generated from RAW traffic passively without any impact of device performance and pushed to Collector (separate server). C-DOT has also developed an IPFIX probe which can be deployed in such a way that it does not have any effect on device utilization. Therefore, this method can also be used for IPDR generation for the scenarios of higher volume of Internet traffic.

4. C-DOT IPFIX Probe:

C-DoT's IPFIX probe can generate flows with Source IP, Source Port, Destination IP, Destination Port, Flow Start Time, Flow End Time, Byte Counts, Packet Count, TCP Flags etc. for IPv4 and IPv6 which can be collected by an ISP on a separate collector server and required files can be

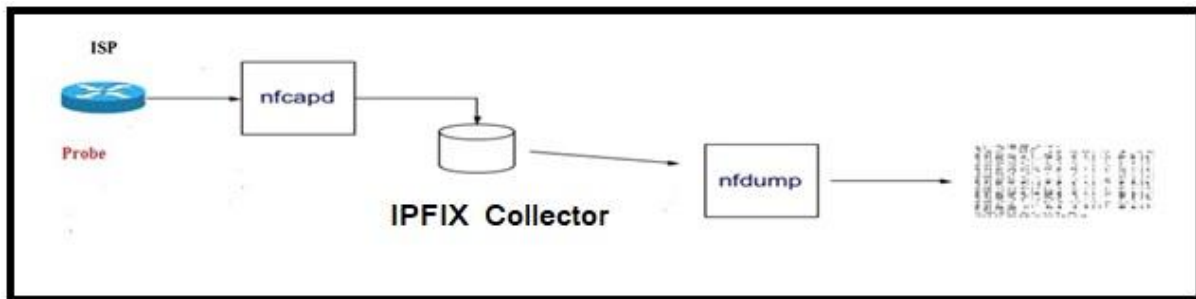
retrieved by invoking customized scripts as per requirement. Assuming that other required logs and sufficient storage space are available with ISP, these logs can provide IPDR access records.

IPDR logs can be generated by C-DOT IPFIX probe as shown in sample schematic below:



4.1 IPFIX Flow Collection

Netflow / IPFIX Flows are exported from network device / C-DOT IPFIX probe and can be collected on some server called IPFIX Collector wherein Daemon “nfcapd” listens on specific UDP Port to collect and save exported flows data into files as per defined intervals.



Flows are collected on collector by invoking following command (Interval and destination directory can be defined)

```
# nfcapd -p 3000 -M flowname -D
```

4.2 Reading Flows: NFCAPD

- NFCAPD receives the IPFIX Flow data from the network and stores the data into files. Automatically rotate files at defined interval.
- Needs one nfcapd process for each flow stream.
- Sample data is shown below for reference.

```
root@Kafka1:~/nfdump/rcom/192-168-144-60# ls
nfcapd.202204270955 nfcapd.202204271310 nfcapd.202204271625 nfcapd.202204271940 nfcapd.202204272255
nfcapd.202204271000 nfcapd.202204271315 nfcapd.202204271630 nfcapd.202204271945 nfcapd.202204272300
nfcapd.202204271005 nfcapd.202204271320 nfcapd.202204271635 nfcapd.202204271950 nfcapd.202204272305
nfcapd.202204271010 nfcapd.202204271325 nfcapd.202204271640 nfcapd.202204271955 nfcapd.202204272310
nfcapd.202204271015 nfcapd.202204271330 nfcapd.202204271645 nfcapd.202204272000 nfcapd.202204272315
nfcapd.202204271020 nfcapd.202204271335 nfcapd.202204271650 nfcapd.202204272005 nfcapd.202204272320
nfcapd.202204271025 nfcapd.202204271340 nfcapd.202204271655 nfcapd.202204272010 nfcapd.202204272325
nfcapd.202204271030 nfcapd.202204271345 nfcapd.202204271700 nfcapd.202204272015 nfcapd.202204272330
nfcapd.202204271035 nfcapd.202204271350 nfcapd.202204271705 nfcapd.202204272020 nfcapd.202204272335
nfcapd.202204271040 nfcapd.202204271355 nfcapd.202204271710 nfcapd.202204272025 nfcapd.202204272340
nfcapd.202204271045 nfcapd.202204271400 nfcapd.202204271715 nfcapd.202204272030 nfcapd.202204272345
nfcapd.202204271050 nfcapd.202204271405 nfcapd.202204271720 nfcapd.202204272035 nfcapd.202204272350
nfcapd.202204271055 nfcapd.202204271410 nfcapd.202204271725 nfcapd.202204272040 nfcapd.202204272355
nfcapd.202204271100 nfcapd.202204271415 nfcapd.202204271730 nfcapd.202204272045 nfcapd.202204280000
nfcapd.202204271105 nfcapd.202204271420 nfcapd.202204271735 nfcapd.202204272050 nfcapd.202204280005
nfcapd.202204271110 nfcapd.202204271425 nfcapd.202204271740 nfcapd.202204272055 nfcapd.202204280010
nfcapd.202204271115 nfcapd.202204271430 nfcapd.202204271745 nfcapd.202204272100 nfcapd.202204280015
nfcapd.202204271120 nfcapd.202204271435 nfcapd.202204271750 nfcapd.202204272105 nfcapd.202204280020
nfcapd.202204271125 nfcapd.202204271440 nfcapd.202204271755 nfcapd.202204272110 nfcapd.202204280025
nfcapd.202204271130 nfcapd.202204271445 nfcapd.202204271800 nfcapd.202204272115 nfcapd.202204280030
nfcapd.202204271135 nfcapd.202204271450 nfcapd.202204271805 nfcapd.202204272120 nfcapd.202204280035
nfcapd.202204271140 nfcapd.202204271455 nfcapd.202204271810 nfcapd.202204272125 nfcapd.202204280040
nfcapd.202204271145 nfcapd.202204271500 nfcapd.202204271815 nfcapd.202204272130 nfcapd.202204280045
```

4.3 –ProcessingNetFlow / IPFIX Flows:

Process Flows: NFDUMP

- Process NFDUMP Processes collected records.
- View the desired fields like Source IP, SourcePort, Destination IP, Destination Port, Flow Start Time, Flow End Time etc, from the stored NetFlow/ IPFIX data files.
- Output of this process are IPDR records.
- Sample records are shown below for reference.

```
root@Kafka1:~/nfdump#
root@Kafka1:~/nfdump#
root@Kafka1:~/nfdump# nfdump -R rcom -o "fmt:%ts %te %sap-> %dap" -t 2022/04/27.11:30:00-2022/04/27.11:35:00|more
Date first seen      Date last seen      Src IP Addr:Port    Dst IP Addr:Port
2022-04-27 11:30:00.000 2022-04-27 11:30:00.002 220.225.205.97:17508-> 142.250.192.36:443
2022-04-27 11:30:00.000 2022-04-27 11:30:00.003 220.225.205.97:57037-> 142.250.76.170:443
2022-04-27 11:30:00.000 2022-04-27 11:30:00.002 220.225.205.97:11643-> 142.250.76.170:443
2022-04-27 11:30:00.000 2022-04-27 11:30:00.002 220.225.205.97:36170-> 142.250.76.170:443
2022-04-27 11:30:00.018 2022-04-27 11:30:00.020 115.249.248.177:57322-> 173.194.14.169:80
2022-04-27 11:30:00.037 2022-04-27 11:30:00.043 35.244.208.123:443 -> 115.248.43.70:57699
2022-04-27 11:30:00.049 2022-04-27 11:30:00.049 220.225.149.151:57117-> 172.217.166.174:443
2022-04-27 11:30:00.024 2022-04-27 11:30:00.053 115.249.232.45:59879-> 40.99.9.162:443
2022-04-27 11:30:00.028 2022-04-27 11:30:00.057 121.240.7.5:443 -> 115.248.50.67:53323
2022-04-27 11:30:00.007 2022-04-27 11:30:00.066 3.111.231.51:44556-> 220.226.189.166:443
2022-04-27 11:30:00.007 2022-04-27 11:30:00.066 3.111.231.51:44558-> 220.226.189.166:443
2022-04-27 11:30:00.058 2022-04-27 11:30:00.067 115.249.206.253:64960-> 13.107.138.9:443
```

5. Implementation Scenario- 1: ISP sites installed with C-DOT Internet Monitoring System (IMS)

- (i) IPDR data(Source IP, Source Port, Destination IP, Destination Port, Flow Start time, Flow end time etc.) can be generated by deploying C-DOT IPFIX probes at ISP gateway location.
- (ii) These flows can be collected on a separate server installed locally / remotely and can be saved in some directory on server based on some pre-defined interval by the ISP.
- (iii) It will require appropriately sized server(s) to collect and save the flows.
- (iv) Required IPDR records can be retrieved from saved flows by applying customized filters as and when required.
- (v) This method will provide Source IP, SourcePort, Destination IP, Destination Port, Flow Start Time, Flow End Time, Byte Counts, Packet Count, TCP Flags etc. for IPv4 and IPv6.
- (vi) No NAT logs are available in this method as IPFIX flows are generated on traffic TAPed at gateway.
- (vii) Correlation with subscriber databasemay be done with the help of existing solution.

5.1. IPDR Parameters (for IPv4/IPv6) available with IPFIX

S.N.	Parameters	Remarks
8	Source IP address with source port	YES
9	Static/ Dynamic IP address allocation	ISP has the information
10	Destination IP with destination port	YES
11	IST Start Time of IP address allocation (hh:mm:ss)	Communication Start Time
12	IST End Time of IP address allocation (hh:mm:ss)	Communication End Time

6. Implementation Scenario2: ISP sites not installed with Internet Monitoring System (IMS)

Option (i)

Netflow can be configured on Network devices. However, Flow generation sampling rate varies from devices to device. The device capabilities for NetFlow generation can be confirmed by respective OEM. Many of enterprise grade devices now support 1:1 Netflow generation. This will provide IP access metadata including destination IP and destination port. Other related subscriber database(s) may be used to generate IPDR in required format as is being done currently to provide IPDR as per guidelines issued in 2013.

Option (ii)

Syslog can be configured on Firewall or Integrated Router network devices. These logs can be transferred to a separate log server and then customized scripts can be used to retrieve required information from logs. Logs can be stored / transferred at some defined interval on a log server as per requirements. Other related subscriber database(s) may be used to generate IPDR in required format.

Option (iii)

C-DOT IPFIX probe: This will require installation of TAP device for getting a copy of traffic and Load balancer for aggregation of traffic. IPFIX probes will generate the IPDR using IPFIX flows. These flows can be collected on a separate server installed locally / remotely and can be saved in some directory on server based on some pre-defined interval. It will also require appropriately sized server(s) to collect and save the flows. Required IPDR records can be retrieved from saved flows by applying customized filters as and when required. This method will provide Source IP, Source Port, Destination IP, Destination Port, Flow Start Time, Flow End Time, Byte Counts, Packet Count, TCP Flags etc. for IPv4 and IPv6.

No NAT logs are available in this method as IPFIX flows are generated on traffic TAPed at gateway. Any NAT logs may be correlated with logs of actual NATing device. Other related subscriber database(s) may be used to generate IPDR in required format as is being done currently to provide IPDR.

7. Conclusion:

ISPs can use any of the method like syslog generation in Network Device , NetFlow generation (after confirmation from OEM about flow generation sampling rate) , CDOT IPFIX probe to generate IPFIX flow. The logs/flows may be collected on a separate server and necessary information may be retrieved using customized scripts for IPDR generation.

However other logs like NAT / AAA / IP address allocation etc. are also required to be correlated with the relevant databases as is being done currently for generation of IPDR format issued in year 2013. The Licensees may consider the solutions based on their own assessment to timely implement the revised IPDR format issued by DoT vide letter dated 16.1.11.2021.

Annexure: 1

Government of India
Ministry of Communications & IT
Department of Telecommunications
Sanchar Bhawan, 20 - Ashoka Road, New Delhi-110001
(Data Services Cell)

No. 820-01/98-LR/Vol.(IX) Pt..I

Dated : 01.10.2013

To
All Internet Service Providers
All UASL/CMTS/UL(AS)/UL Licensees

Subject : Parameters for Internet Protocol Detail Record (IPDR) and SYS LOG of Network Address Translation (NAT)

The Internet Protocol Detail Record (IPDR) format for Internet and GPRS Services and Parameters to be stored for SYS Log of Network Address Translation (NAT) have been finalized.

2. The Internet Service Providers and the UASL/CMTS/UL(AS)/UL Licensees are hereby directed to maintain log for the following parameters with immediate effect:

(i) IPDR Parameters to be stored in respect of Internet and GPRS Services:

Sr. No.	Parameters
1*	Name of person/organization
2*	Address
3	Contact No.
4**	Alternate Contact No.
5**	E-mail Address
6	Landline /MSISDN/ MDN /Leased circuit ID for Internet Access
7	User ID for Internet Access based on authentication
8	IP address assigned
9	Static /Dynamic IP Address Allocation
10	Source port of the public IP Address in case of NATING
11	IST Start Time of IP address allocation (hh:mm:ss)
12	IST end Time of IP address allocation (hh:mm:ss)
13	Start Date of IP address allocation(dd/mm/yyyy)
14	End Date of IP address allocation(dd/mm/yyyy)
15***	Source MAC Address / Other device Identification number

(Sr. 1 to 5 above may be stored from Customer Acquisition Form (CAF))

(* - Photo ID & Address Proof are required to be maintained separately by the Service Providers)

(** - Optional)

(*** - In place of customer device MAC address, virtual MAC Address of DSLAM/routing device is captured in some of the systems.)


- (ii) Parameters to be stored in SYS LOG of Network Address Translation (NAT) for Internet Access:

Sr. No.	Parameters
1	Start Date (mm:dd:yyyy) & Time (hh:mm:ss)
2	End Date (mm:dd:yyyy) & Time (hh:mm:ss)
3	Source IP Address
4	Source Port
5	Translated IP Address
6	Translated Port
7	Destination IP Address
8	Destination Port

- Term SYSLOG here refers to Logs for Network Address Translation.
- Aforesaid parameters shall also be applicable for NAT mechanism for Dual Stack in IPv6 Network.

3. Internet Service Providers and UASL/CMTS/UL(AS)/UL Licensees shall communicate to their subscriber, other than individual subscribers for recording and maintaining of NAT SYS Log Parameters as mentioned in Para 2 (ii) above for any NAT mechanism deployed by them for access of Internet over the Internet connectivity. The Service Providers shall also obtain the compliance from them in this regard.

Compliance may kindly be communicated immediately.


01.10.2013
(S.T. Abbas)

Director (DS-II), DoT

Annexure: 2

Government of India
Ministry of Communications
Department of Telecommunications
Sanchar Bhawan, 20, Ashoka Road, New Delhi-110001
(Data Services Cell)

No 8520-01/98-LR/Vol.(IX) Pt.I

Dated: 16.11.2021

To

1. All Internet Service Providers
2. All UASL/CMTS/UL(AS)/UL Licensees

Subject: Parameters for Internet Protocol Detail Record (IPDR) and SYS LOG of Network Address Translation (NAT)

Internet Protocol Detail Record (IPDR) format for Internet (Wireless and Wire line) Services and Parameters to be stored for SYS Log of Network Address Translation (NAT) issued vide letter no No 8520-01/98-LR/Vol.(IX) Pt.I. dated 01.10.2013 are hereby revised as per the details given below.

2. The Internet/Telecom Services Providers and the UASL/CMTS/UL(AS)/UL Licensees are hereby directed to maintain log for the following parameters with immediate effect.
 - (i) IPDR Parameters (for IPv4/IPv6) to be stored in respect of Wireless/Wire line Internet Services:

Sr. No.	Parameters	Remarks
1	Name of person/organization	Photo ID & Address Proof are required to be maintained separately by the Service Providers
2	Address	
3	Contact No.	Optional
4	Alternate Contact No.	
5	E-mail Address	
6	Landline/MSISDN /MDN/Leased circuit ID for internet Access	
7	User ID for internet Access based on authentication	
8	Source IP address with Source Port *	Refer note (b) for NATing
9	Static/Dynamic IP Address Allocation	Whether Static/ Dynamic
10	Destination IP with destination port*	Refer note (b) for NATing
11	IST Start Time of IP address allocation (hh:mm:ss)	
12	IST end Time of IP address allocation (hh:mm:ss)	In case of dynamic IP allocation or change of IP
13	Start Date of IP address allocation (dd/mm/yyyy)	



14	End Date of IP address allocation (dd/mm/yyyy)	In case of dynamic IP allocation or change of IP
15	Source MAC Address/IMEI/ Other device Identification number	in place of customer device MAC address, virtual MAC address of DSLAM/routing device is captured in some of the systems
16	IMSI and SIM type	Only in case of Mobile, IMSI and type of SIM (Physical or e-SIM) to be stored

Note: a. Sr. No. 1 to 5 above may be sourced from Customer Acquisition Form (CAF)

b. ***In case of Private IP address, SYS LOG and NAT details as per 2(ii) are also required.**

(ii) Parameters to be stored in SYS LOG of Network Address Translation (NAT) for Internet Access:

Sr. No.	Parameters
1	Start Date (mm:dd:yyyy) & Time (hh:mm:ss)
2	End Date (mm:dd:yyyy) & Time (hh:mm:ss)
3	Source IP Address
4	Source Port
5	Translated IP Address
6	Translated Port
7	Destination IP Address
8	Destination Port

Note: a) Term SYSLOG here refers to Logs for Network Address Translation.

b) Aforesaid parameters shall also be applicable for NAT mechanism for Dual Stack in IPv6 Network.

3. Internet Service Providers and UASL/CMTS/UL(AS)/UL Licensees shall communicate to their subscriber, other than individual subscribers for recording and maintaining of NAT SYS Log Parameters as mentioned in Para 2 (ii) above for any NAT mechanism deployed by them for access of Internet over the Internet connectivity. The Service Providers shall also obtain the compliance from them this regard. The revised IPDR format will come into effect w.e.f 31.03.2022.


 16/11/21
 Director (DS-II), DoT
 Phone: 011-23036860