Efficient Monitoring of Network Failure Through RADIUS Servers and External Database

Syed Mansoor-ul-Hassan Bukhari

Institute of Communication Technology
Islamabad (ICT)
mansoor.bukhari@ptcl.net.pk

Abstract:

Failure detection and resolving problem before the customer register complaint remains an unresolved issue for a service provider and telecom companies. Access and aggregation networks plays vital role in extending uninterrupted and QOS to end users for which efficient monitoring is an important factor that cannot be neglected. Standard monitoring servers commercially available are either product specific or have limited features and are not capable enough for auto detection of important type of failures that can help in instant recovery.

In this article, best design for failure discovery is proposed which is based on data analysis in real time using Remote Authentication Dial-in user server and external database that captures all events of Point-to-Point session disconnection.

An algorithm is applied for detection and notification of failures at any network element through a centralize location for rapid recovery. RADIUS feed is sent to external database and analytic system in real time to avoid any computational load, performance issues on RADIUS servers and to achieve high level of efficiency. It also helps operators to diagnose problems before the customer's register complaints through helpline. Once the rapid recovery is done and services of customers are reinstated in less time, it may help an operator in controlling the churn rate, increases customer satisfaction, reducing customer complaints and ensuring that quality of service committed to the customer is achieved.

Keywords: RADIUS, DSLAM, BI, OSS, Network, Monitoring, AAA, QoS, Database, Failures

INTRODUCTION

1.1 Monitoring

Monitoring plays a key role in providing uninterrupted and committed services to the customers. Telecommunication operators has to bear huge cost in deploying various type of solution to monitor different resources in their network. It is also evident that in a small or big enterprise there is not a single solution available which has enough capabilities to monitor all the different problems from a centralized location. Every vendor deploys his own monitoring solution which can only monitor devices that are of the same make or supported by vendor (property devices). In operators where multiple vendor products are running it is also noticed that for each vendor they have different type of network management systems. NMS is responsible to manage vendor supported devices from a common location and notify different types of alerts on it graphical user interface. The operator also has to manage different type of NMS in their network. Due to this segregated nature and distributed management sometime it is quite difficult for an operator to proactively respond to outages as alerts remained unattended or not acknowledged in timely manner and they are overlooked or ignored. It is also observed that vendor specific management systems are only capable to monitor pre-defined dataset of configured alerts and they are not meant for managing problems that are not configured like issues that occur often in the network such as bulk disconnection of subscribers.

To address such type of problems operators are using various types of 3rd party products with them extra cost is associated or open-source monitoring solutions are used like MRTG, Nagios, Cacti, Zabbix or any vendor specific products which further takes it input from different NMS system. The 3rd party solutions although are capable to integrate different vendor types NMS to get the alarms information but still lack in addressing issues which are not reported by NMS itself (like DSLAM or MSAG cards hang).

1.2 Real-time monitoring in cloud computing

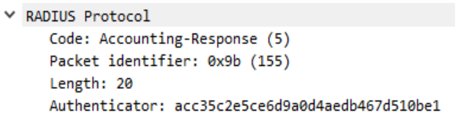
Recently, cloud technology has brought informational technology revolution. A remote real time monitoring system relies on cloud computing that contains cloud monitoring platform and the purpose is to collect data, diagnose a fault and triggering alerts. It contains of monitored terminal, management terminal and cloud monitoring platform. The monitored terminal and the management terminal are connected to the cloud platform though internet. Operation state data is sent to the management terminal by cloud platform whereas the management server through cloud platform sends control data to the monitored server. The cloud based real time monitoring has low cost as the operator has not to buy any additional hardware or bear software cost [17]. Pattern based monitoring can be performed by checking real time or historical data from the logs of network management server that may point issues related to performance, security and increase or decrease in traffic [18].

1.3 Role of RADIUS Servers

RADIUS Protocol is used to transmit information of authentication, authorization and accounting (AAA) between BRAS and RADIUS server. The well-known ports on which the data is carried are 1812,1813 (authentication and accounting respectively) and the transport protocol used is UDP. The BRAS act as a client for RADIUS servers and it is configured to pass through information to different RADIUS servers. On a BRAS different RADIUS servers may be defined in round-robin or if load balancers are used with RADIUS servers then on BRAS primary or secondary model is defined. Whereas, inside the load-balance multiple RADIUS servers can be defined for distribution of requests equally on all the RADIUS servers. The RADIUS servers work on the principle of getting the request from the BRAS (Access-Request) and send back the response (Access-Response) to the client. The connection between the RADIUS servers and the BRAS is secured by configuring the shared-key which is never sent over network.

Once the shared-keys are exchanged and the BRAS is configured to send requests to defined RADIUS servers then the RADIUS server will start processing all the incoming requests. It processes the requests by sending acknowledgment that packet is received. RADIUS server either Accept or Reject the request on the basis of different criteria set for the different type of requests. RADIUS servers can process all incoming request by itself or it can forward the request to external system to get the response back to take decision either to validate request or invalidate the request.

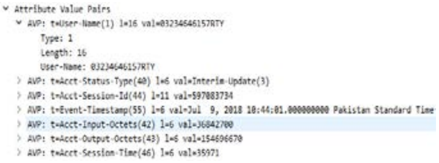
The RADIUS data contains Code field which is one octet, Identifier field is also one octet, Length field is two octets and Authenticator field is sixteen octets. Request authenticator of Access-Request contains User-Password [2] attribute but in Accounting-Request this attribute is not present due to which both authenticators are done in different ways. Accounting-Response code is (5) and Accounting-Request code is (4) if packet contains any invalid code it is discarded. The Figure.1.1 below explains the packet capture of Accounting-Response sent on port 1813.



```
∨ RADIUS Protocol
    Code: Accounting-Response (5)
    Packet identifier: 0x9b (155)
    Length: 20
    Authenticator: acc35c2e5ce6d9a0d4aedb467d510be1
```

Figure.0.1: RADIUS Request sample fields

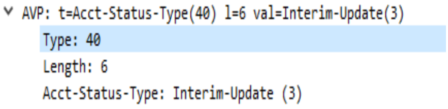
The incoming request or packet contains different attributes. These attributes contain standard RADIUS attributes and vendor specific attributes (VSA) for authentication, authorization and accounting. Attribute can be multi-value based on it requirement and use. The attribute format contains Type, Length and Value fields (Type, Length are one octet and Value can be zero or more octets). Value is more specific to attribute information and it value depends on the type of attribute it can be integer, string or ipaddr. Some values of RADIUS type field are reserved for experimental purpose, implementation purpose and some cannot be used (241-255).



```
∨ Attribute Value Pairs
  ∨ AVP: t=User-Name(1) l=16 val=03234646157RTY
      Type: 1
      Length: 16
      User-Name: 03234646157RTY
  > AVP: t=Acct-Status-Type(40) l=6 val=Interim-Update(3)
  > AVP: t=Acct-Session-Id(44) l=11 val=597083734
  > AVP: t=Event-Timestamp(55) l=6 val=Jul  9, 2018 10:44:01.000000000 Pakistan Standard Time
  > AVP: t=Acct-Input-Octets(42) l=6 val=36842700
  > AVP: t=Acct-Output-Octets(43) l=6 val=154696670
  > AVP: t=Acct-Session-Time(46) l=6 val=35971
```

Figure.0.2: RADIUS attribute value pairs (AVP)

The RADIUS attributes contains very useful information referred to Figure.1.2. The Acct-Status-Type [16] attribute contains information about start of session, end of session and ongoing session having value 1,2 and 3 respectively. Where Acct-Status-Type (40) is reserved to record the status of each session, all vendors have to comply with use this AVP as it cannot be changed or they cannot use it for any other purpose (Figure.1-3)



```
∨ AVP: t=Acct-Status-Type(40) l=6 val=Interim-Update(3)
    Type: 40
    Length: 6
    Acct-Status-Type: Interim-Update (3)
```

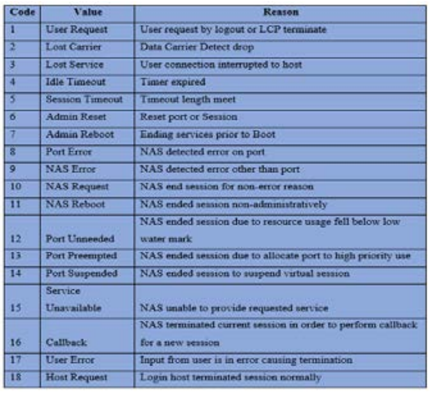
Figure.0.3: Attribute used for distinguishing accounting

In Figure.1.2 the Acct-Input-Octets [16] and Acct-Output-Octets [16] indicates that how many packets received and sent to the port for the ongoing session. This information is only present in the accounting requests when the Acct-Status-Type [16] is Interim or Stop. Acct-Session-Id [16] is one of the important attributes in RADIUS accounting that must be present in the accounting request and has a unique value. The unique value received in this attribute is important and is used to easily track any session in the accounting log files or database (every session has unique value for this field and remains the same till the session is ended).

1.4 RADIUS Termination causes

Similarly, Acct-Termination-Cause is also one of the key attributes indicating the reason due to which a running session was stopped and this attribute is only present in the accounting records when a Acct-Status-Type [16] value 2 is received. When a user session ends there are various type of causes recorded in the logs. This attribute can be used to point-out issues which cannot be detected through standard or available monitoring servers in the market.

Some prominent cause codes are discussed with value and reason in Figure.1.4



Code	Value	Reason
1	User Request	User request by logout or LCP terminate
2	Lost Carrier	Data Carrier Detect drop
3	Lost Service	User connection interrupted to host
4	Idle Timeout	Timer expired
5	Session Timeout	Timeout length meet
6	Admin Reset	Reset port or Session
7	Admin Reboot	Ending services prior to Boot
8	Port Error	NAS detected error on port
9	NAS Error	NAS detected error other than port
10	NAS Request	NAS end session for non-error reason
11	NAS Reboot	NAS ended session non-administratively
12	Port Unneeded	NAS ended session due to resource usage fell below low water mark
13	Port Preempted	NAS ended session due to allocate port to high priority use
14	Port Suspended	NAS ended session to suspend virtual session
15	Service Unavailable	NAS unable to provide requested service
16	Callback	NAS terminated current session in order to perform callback for a new session
17	User Error	Input from user is in error causing termination
18	Host Request	Login host terminated session normally

Figure.0.4: RADIUS Account Termination Causes

The Figure.1.4 and Figure.1.5 explains the type of disconnections that may happen to a user session. The User-Request is due to the reason customer request a logout. Lost-Carrier is associated to the CPE end where data carrier detects a drop. Session Timeout appears when the total time for a session limit is reached and it is disconnected. NAS-Error, NAS-Request are associated to the BRAS. When the BRAS initiates any session disconnection in such cases, the cause code recorded is NAS-Error or NAS-Request.

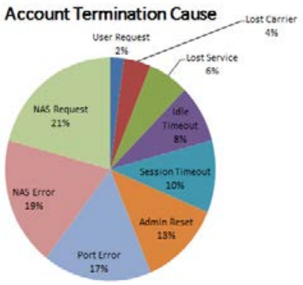


Figure.0.5: PIE CHART - Termination Cause

1.5 PPP over Ethernet (PPPoE)

Point-to-point protocol is commonly used to establish PPP session and encapsulate PPP packets over Ethernet. It is established for providers where there is need to maintain the session associated with broadband access technologies. Also, when there are requirements to connect multiple host through same CPE at any remote location it is used. It enables the service provider to save cost, provide access control and enable per user based billing mechanism.

1.5.1 How Point-to-Point over Ethernet works

The Discovery stage is four steps process including Initiation packet, Offer packet, Request packet and Confirmation packet. When confirmation is received the host proceeds to PPP session stage. The PADI packet is initiated by the host where the destination address is a broadcast address and one tag containing required service must be present. The broadcast is received by multiple server but based on the required service tag the server respond by sending a PADO packet with destination Mac-Address as the unicast address of the host which initiated the PADI packet. In PADO packet server must sent its name and with same required service name tag similar to the one received by it in the PADI packet. It can also send other additional service-name tags which it can offer to the host but a server cannot respond to any request or for any service which it cannot offer to the Host. The initial PADI was a broadcast due to which the Host was responded by several servers. The Host chooses one server name and sends a PADR packet to only that specific server with destination address as the unicast address of the selected server with a code 0X19 and Session_ID as 0x0000. On receiving the PADR packet the server generates a unique Session_ID to begin a PPPoE session and respond to the host with this unique Session_ID, code 0x65 and destination address as unicast address of the host. Finally, if a session is required to be disconnected either the host or server initiates a PADT packet with code set to 0Xa7 and Session_ID info which need to be disconnected. Once PADT is triggered the communication is not allowed using that specific session. During an established session server sends echo-packets to ensure the session state is maintained because in several cases if PADT is not initiated by the host then server will not know the state of session that it has already ended. In PPPoE, the mechanism of re-tries is defined at both the server side and host side. If a PADO is not received by the host with in specified time it will resend the PADI packet for number of tries configured and doubled the time each time. Similarly, if a Host has not received PADS packet the Host should re-send PADR using same timeout mechanism. Once re-tries limit meets PADI packet is resent.

1.6 Scope of work

The scope of this research is based on utilizing information from various systems to overcome problems and limitations like finding actual card capacity of each card of a DSLAM or finding total occupancy of card using provisioning inventory. Once the actual capacity of card or occupancy is known further analysis can be carried out for failure detection within the broadband network. The issues that reside in the network for long duration but remained unattended are discussed and different ways explored for finding, classification and diagnosing a fault. In past there were no prominent research works are carried out in which monitoring is performed using RADIUS as best known to the author.

The use of auto-provisioning (OSS) in a telecom service provider network enhance the visibility and also increase the control for installed network devices. It enables an operator to automate all operations through one system and keep track of all changes made. It is used to automate the port allocation process and it helps to achieve the visibility for status of ports on each network element. Proposed here a real-time monitoring and analytic system that gets its feed from the external database. The accounting processing directly on the RADIUS servers has performance constraints whereas external database is optimized to give better response to searching data from thousand and millions of rows. The external database is further integrated to the BI system that has the capabilities for performing analytics on the input data using the historical data and the present data. On the basis of the available data the system may perform different type of analytics, generate reports and create incidents based on any irregularity found in the user's behavior or trends.

The thesis is distributed into following chapters. In second chapter, recent work is reviewed that is carried out in the field of network monitoring, also explored the kind of techniques available to achieve it. Chapter three sheds light on recent approaches being carried out for network monitoring. The chapter four discusses system model, applied algorithm and methodology is discussed in detail using it may help service providers and telecom operators to formulate one consolidated solution for several thousand network elements monitoring without applying any change to their existing network. In chapter five different results are extracted from a production environment that points to different types of problems that existed and remained unresolved for several days. The conclusion and scope of the future implementations is also presented at the end.

1.6.1 Problem Statement

Failure in networks causes a number of customers to suffer. In several cases, service providers are unable to diagnose a problem well in time, before it is escalated through a customer complaint, the failures that happened and remained unattended cause huge revenue loss to the service provider and customers may unsubscribe services. The customers prefer providers which provide stable and better quality of service (QoS). The main focus of this research is to find problems that resides in the network but are silently resolved, are unnoticed and service level agreements are not taken into consideration and customers experience long duration outages. In mostly cases vendors are responsible for managing equipment's of their own make and on different devices covered under some support contract. Recently, there was a solution proposed to detect mass PPPoE failure in a network using RADIUS servers [1]. Two search criteria used were on the basis of card capacity and occupancy of card but it had some limitations like capacity of card was not known. There is one other work carried out for monitoring state of PPP session [14] using RADIUS servers for a network element but it also not addressed issues up to cards or ports within a network element. The stated above problem and limitation is addressed in this research work.

MONITORING SYSTEMS

1.1 Network Management System

There is also a US patent [19]. The patent explains network management system that maintains inventory in which data is stored for a respective network resource present in the network. Order entry is basically a change request that specify an update made to the network. Network inventory is updated in response to the initiated request. Several adopters are used to access components through which update or modify is carried out at inventory level or network element as explained in Figure.2.1.

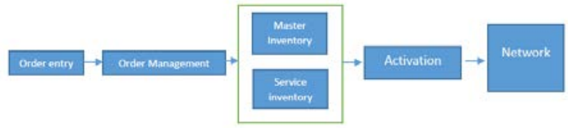


Figure.2.1: Automated network updates using NMS inventory

Network inventory maintains records for network element installed and their connection information. Network discovery is sometime also used to obtain the information from the network automatically but doing so cannot ensure the actual installed based in the network and it can disrupt the process of service provisioning in a network. Most recent provisioning system contains an inventory database for building up inventory for network resources. This ensures that if any modification is required the network inventory is first updated and then configuration to be updated at the network element for which the change request is initiated. The process also ensures that configuration is consistent at inventory and network. It also ensures efficient automation for all other processes which use inventory (service provisioning, modification required at network). The network inventory contains both physical and logical resources. The logical resources deal with logical port and bandwidth modification. Inventory update component is capable to execute a specific stored script based on the change request. The use of different scripts specifies its own modification action that simplify a CR. The CR can be related to external element where the modification is required on external system over the network, doing so has increased the efficiency and flexibility for network level changes. Single configuration action can perform multiple modifications due to which network trouble can be evaded

Service inventory is linked to the master inventory and is responsible for provisioning of services at network level. Similarly, to network inventory, service inventory is being used for updating configurations and sending them to the network resource so that a specific service can be enabled at the network element. The master inventory is used to keep the service inventory updated or it can be a single network inventory stored as specified data model in the database.

1.2 Auto-Provisioning

In Telecommunication service providers rely on operational support system due to raise in the number of services and products offered to the customers. The OSS enables an operator to perform operations on multi-vendor hardware and software systems. It may include different telephony components, network interfaces, data network and process manager. The time to market is reduced due to enhancement in modules through use of Java code, XML, JSP, HTML, C++ in objected oriented style. The service bundling and templet creation has enhanced the functionality as it requires less time for enabling different components in a network and easy to manage for an operator. A user in a single sign-in can have access to different components from where he can trigger various operations like modify, delete, request new service, change network, reporting functionality and tracking things in real-time. At network elements different operations can be performed using network interface in real time like port creation, profile assignment or activation/deactivation of ports. Similarly provisioning system has the capabilities to perform various operations at database level like insertion, updating or deleting of user account.

2.1.1 Use of Provisioning System

In service provider network operational support system plays a vital role in automation of services. The simple provisioning also, represented in Figure.2.2, includes.

- Commissioning of DSLAM/MSAG
- Creating a Port Plan
- Vetting Port plan before adding to inventory
- Loading vetted port plan to OSS inventory
- Provision of services at NE level and user's creation at AAA level

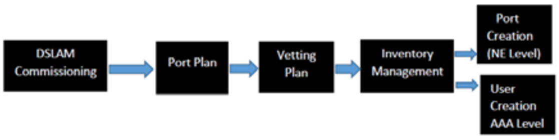


Figure.2.2: OSS steps for automatic provisioning

Provisioning system is helpful to obtain the information about network element total installed base. It gives information for already running network elements, models, vendor type, number of frame, slot, ports and state of ports. On the basis of available inventory different data can be filtered like available cards on each network element, total number of ports available on the card, used ports and not user ports. At the time of commissioning of a new site the port plan is created on the basis of available ports and physical installed subscriber's cards. The port plan is vetting before loaded information to the inventory management system. Initially in the loaded port plan, the ports are not occupied and are free or spare. Once the provisioning is stated the port status is updated at provision end from free to occupied for ports on which new customers are provisioned (Port allocation process). Once the port is occupied it is now not in spare state and provision inventory is automatically updated at the time port is reserved by a system. The provisioning inventory keeps on updating itself on the basis of allocation, removal of ports, blocking of faulty ports and temporary suspending of ports.

The provisioning system performs many operations on a subscriber. It initiates a change request (CR) and an update is sent to the respective NE and also to the database. If addition of a new customer is required, the provisioning system first allocate the resources to a customer from resource inventory of provisioning system and the system selects the network element on which the customer will be provisioned. The provisioning system established a connection to the NMS of the respective vendor and configures the port, in parallel the customer creation information is sent to the external database by the provisioning system to create a new customer in the database.

2.3 Use of External Database

The provisioning system uses the external database to create, delete, suspend or resume the provisioned customer. This information is written to the authentication table which is used by RADIUS servers at the time of authentication requests. The RADIUS server connects the external database through a configuration file available on RADIUS server using connection interface and call a specific procedure. The authentication procedures are maintained in the external database and when they are called they perform different checklists by accessing different tables of the DB. If the procedure is executed successfully response is sent back to the RADIUS server on the basis of this response RADIUS servers either accept or reject the requests. If a subscriber is temporary closed the provision system send a request to external database to change the status of user from enable to disable (1 to 0). The external database authentication table is linked to the provisioning system so that both system remained in sync.

The external database is also used to record different type of accounting information for all the subscribers provisioned in the database. This information is sent to external database by RADIUS servers. The accounting information is stored in the accounting tables. The RADIUS severs configuration files manages different type of accountings for external database (how to send different type of accountings to different tables created in the external database)

The external database is also used to calculate the exact number of ports in service. Using external database also helps to cater and overcome card capacity issues. The card either has 32 to 74 ports and on each port one PPPoE session can be established. If the actual number of ports in service are known the threshold proposed by Zych [1] can be easily enhanced.

2.4 Business Intelligence and In-memory analytics

The integration of BI with other system itself important to achieve success for business intelligence. Using BI capabilities for decision making enables an organization to gain benefit from its BI investment. [20]. BI has the ability to accurately deliver information to the users which enables the organizations to increase business and achieve business liveliness. A separate analytical data warehouse can accept data in real time from different systems in a database which also has the capabilities of analytics in virtually real time. In memory systems are easy to use, present efficient reports and help users in timely decision making. It also has analytical database that is capable of taking useful information from operational database and applying analytics using it.

The real-time queries required to be executed against up-to-date subscriber data based on which instant reports are created. The interactive dashboards and to carry out spontaneous jobs low response time and rapid results are desirable. This has been made possible by using in-memory analytics [21]. Real time access of BI to an enterprise for everyone in important that can be inserted in many business systems. It has also growth potential whereas Microsoft has clear policy of driving business intelligence in their office suite. Recently live business intelligence has changed reporting to transport data-intense, real time analytics for BI functions in a growing enterprise. Therefore, BI is considered as a unified data and analytics platform that present quality and predictive analytics in real-time. The use of BI technology is very common in different enterprises as it has use for manufacturing, retail, financial services and telecommunication sector. The data on the basis of BI performs analysis can be gathered from different sources that are reconciled.

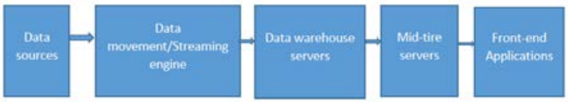


Figure.2.3: BI real time analytics

2.5 Big Data Platform

Data lake has enabled organizations to a magnitude that they can now store data in much bigger diversity and size without having to care about database schema. In addition, it has changed the way organizations used to derive their insights. Data lake provides the company an added advantage since the central repository holds the capability to contain any type of data be it structured or non-structured, therefore enables one from the worry of schema design. Since data lake has the ability to hold any type of data, so it enriches operator to perform advanced analytics (machine learning, predictive analysis) in addition to uncovering insights from historic data.

DEEP LEARNING

3.1 Challenges in Broadband Services

Broadband services when disconnected are challenging to diagnose. The disconnection in the connectivity means that there will be no data communication on the broadband line. The network device terminating at the network side of a DSL connection may be a DSLAM, OLT, MSAG or Access Node. Due to several reasons, the broadband connection is unable to communicate to the network management device that could be due to physical cable break in the cable on which the broadband connection communicates, malfunction of the CPE or any type of wrong configurations [5].

3.2 Type of DSL technologies

The DSL or xDSL technologies provide transmission of digital data over the wires of the telephone network. There are various xDSL technologies used in an ISP for the purpose of extending high speed internet services to the customers. Some of the common used xDSL technologies are ADSL G.992.1, ADSL2plus G.992.5, VDSL2 G.993.2, vectored VDSL2 G.993.2/G.993.5. The ADSL2plus supports up to 16Mbit/s whereas vectored VDSL2 can provide 100Mbit/s. [6]

3.3 Passive Monitoring

There is another US Patent [7] who has proposed a monitoring solution for a huge network. The solution is based on the passive monitoring for network issues. For the network to be monitored initially network taps being placed for replicating traffic to a switch and tire 2 switches analysis computing devices. It analyzes frames and used statistics to resolve issue by removing additional flow table entries if required. This solution is related to layer-2 based monitoring and no monitoring is carried out at the upper layer of the network.

3.4 Monitoring a resource remotely

There was another patent [8] who presented a method and tool for the purpose of fault detecting in a network. It considers network termination device that helps in pointing out the problem in the portion of the link between device and BRAS which can include the copper lines too. It may collect a statically significant sample of customers CPE and remotely monitor its connectivity during defined intervals and find out average level of connectivity. It applies rules to interpret variations and if any variations are found it determine the fault location from the physical and logical network topology. It also prompts alert and resolves the fault. This proposed solution is limited to CPE fault management and it does not cover overall monitoring. Whereas, the applied algorithm in this work has the visibility of all the behaviors of CPEs and it can also be deployed for monitoring connectivity variation for any CPE using the CPE Mac-Address which is also available in the accounting logs stored in the external database.

3.5 Monitoring quality of a DSL Line

To determine the quality of digital subscriber, line another US patent [9] proposed a method for management of DSL. The signal to noise ratio is continuously measured for a DSL line by comparing it to the SNR margin of a better lines. If the line SNR is low, the line test is initiated in the electrical domain and for improved method where atmospheric moisture level can be measured used moisture level sensors. The quality of line good or bad can also be measured using the model applied in my research work. The users which are disconnected more frequently may fall under the line related issues on which further analysis can be down using the RADIUS accounting logs available in real time to different systems that are responsible for taking data in the real time and analyze them.

3.6 Challenges for RADIUS logs monitoring

The network traffic has increased over the past and the latest network devices are comparatively more complex from old devices. A network generation tool is useful for testing in-line networking devices. It is useful to find out the traffic behavior but control for traffic generation is very challenging [4]. Applying extra processing like fetching accounting logs in run-time from RADIUS server when it has to process millions of transactions per day may result into performance issues due to exponential growth in traffic on daily basis. In this research work it has been handled through performing all such processing out of the RADIUS servers instead of any processing directly on the servers.

3.7 Security of RADIUS Protocol

RADIUS protocol has strong authentication scheme that enables centralized authentication, authorization and accounting for all users who want to connect and user network services. Unique encryption for every single session is applied that prevents other users for gaining access to sensitive information. Each client can be effortlessly unauthorized if the unique encryption key is updated or regenerated. It protects the users from accessing the network and also secures the user access to other security keys of different clients. Different type of network permissions like firewall polices, quality of service or any kind of scheduling can be associated to user profiles on the bases of their identities. [10]

3.8 Model for existing Network Monitoring

To increase the revenue based on services extended to the customers from different solution used by a telecommunication operator in the era of close competition more efforts are required for increasing the satisfaction level and their loyalty. [11]

The author [12] focuses on the existing network monitoring. The network management operation phase consists of design, development and monitoring phase. It emphasizes on technologies for network monitoring that are further classified in to five different categories. The data is growing with the growth in the network due to this reason more struggles required for enhancing monitoring. Measurements and configuration are presented in a way that monitoring operations gathered current statistics in order to deduce the existing behavior of a network. Any change in the configurations is carried out by design operations whereas the deployment operations is responsible for implementing the planned changes in the network. The monitoring operations is responsible to observe that the behavior is same as expected and it does not change.

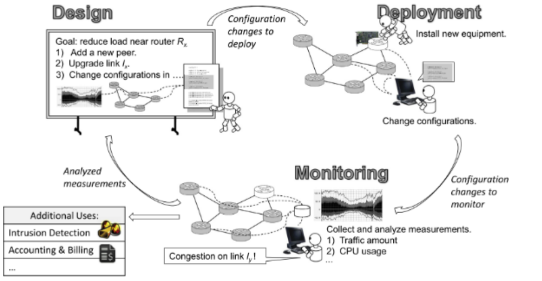


Figure.3.1: Different phases for network management

Further the monitoring operation uses a model for the purpose of knowing the state of network, troubleshooting and future planning. The proposed work in the paper is more focused on the network layer based monitoring, while the solution discussed in my research work is capable to point-out any issues with specific network device and alarm may be triggered in the case the client stops sending requests or triggered huge disconnections.

There is another monitoring solution presented, as due to busy life continuously monitoring a resource by user himself is not possible for this reason alert triggering through SMS is the more convenient option. The information stored in embedded Webserver generates a message to the client or triggered an alert and the data to the client is accessible in real time. [13]

3.9 PPP session based Monitoring using a Management device

A US patent [14] worked on the collection of data for a PPP session where the measuring device is configured to automatically establish a PPP session with the BRAS and the RADIUS server. The collection of data for a PPP session is from the RADIUS server. The management device is placed in the central office on a port of DSALM and it connects automatically a PPP session on the BRAS. Using the RADIUS server accounting logs, the session time start, information is collected by the data collector at the NOC and aggregates RADIUS data for the purpose of checking network connectivity. The research work is more focused on the monitoring of the network element itself instead of digging inside of the access elements specific issues related to cards or ports. In my opinion, it is also one of the close research being carried out for monitoring state of PPP session using RADIUS servers but it may lack the phenomena of using accounting causes and correlation of data that is covered in my research work.

3.10 Use of Dynamic Line Management

There is another US patent [15] he used a management device like dynamic line management (DLM) that is responsible for collecting data from end devices and device like DSLAMs/MSAGs. The DLM profiles contains set of values for different parameters linked with the data connection. Applying DLM profile to a connection is dependent on monitored data output and pre-defined profiles parameters values and this implementation of new profiles is automated using the provisioning system. This solution is more inclined to fixing the problematic lines but is not capable to tell the duration of faults and how many times it has occurred. It may be limited in the case the services on the ports are down or in the case of frequent card reset issues. This limitation is covered in my research work and OSS data is used more efficiently for the purpose of knowing exact statistics of a network resource and applying correlation of data from different sources for monitoring more problems that are not covered but independent solutions.

SYSTEM MODEL

The model proposed here is developed through integrations of different systems including the provisioning system (OSS), RADIUS servers, External database (DB) and Business intelligence (BI) system. This system model is used to address all limitations in previous work by Zych[1]. The model also addressed the performance issues on RADIUS servers in the case of high load and enhance the efficiency of fault detection through external systems in real time.

4.1 Systems involved in Monitoring

The total card capacity for network elements in a network is not known. Generally, card has ports between 16 to 74 and till now no one has addressed the card capacity problem and mechanism to figure out used ports or free ports. The provisioning system used here is helpful in automation of different tasks for any service provider. One of the essential part of provision system is building its own inventory. When any new network element is provisioned, the inventory is updated accordingly and service provisioning modules can be used from single system to carry out automated provisioning on all the available network elements in the network. The Figure.4.1 shows basis integration elements for fault detection and performing analytics.

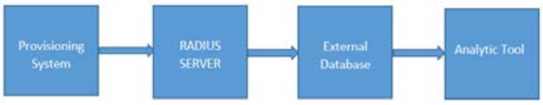


Figure.4.1: Proposed model for efficient monitoring using RADIUS feed

The flow in Figure.4.2 explain how a new provisioning takes place on a network element and whose domains are involved in the process of auto provisioning. The provisioning mechanism explained in below figure tells how the flow is dependent on different domains and to achieve automation of network elements the process starts from the commissioning of any new site it includes verification process by business team, loading of port plan, updating port inventory, creating a new NE group and updating interconnected systems.

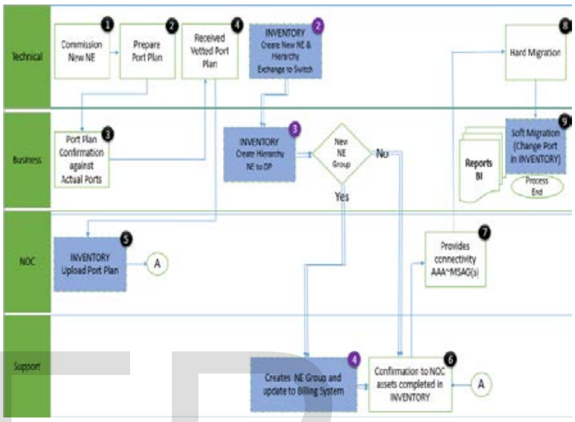
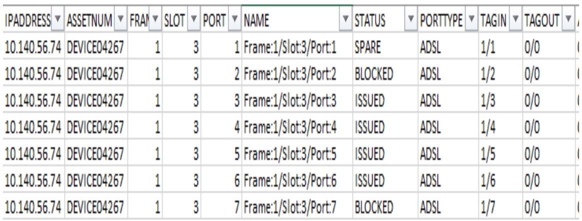

Technical
Business
NOC
Support
1
Commission New NE
2
Prepare Port Plan
4
Received Vetted Port Plan
2
INVENTORY Create New NE & Hierarchy Exchange to Switch
8
Hard Migration
3
Port Plan Confirmation against Actual Ports
3
INVENTORY Create Hierarchy NE to DP
New NE Group
No
Yes
Reports BI
9
Soft Migration (Change Port in INVENTORY)
Process End
5
INVENTORY Upload Port Plan
A
7
Provides connectivity AAA^MSAG(s)
4
Creates NE Group and update to Billing System
6
Confirmation to NOC assets completed in INVENTORY
A

Figure.4.2: Auto-provisioning flow for an ISP

Initially, to commission a new NE, the port plan is prepared. The port plan contains some important information like;

- Unique IP Address of the NE
- Frame information of MSAG/DSLAM (Logical card information)
- Slot information of MSAG/DSLAM (Physical/Logical card information)
- Port of the MSAG/DSALM (Physical/Logical card information)
- Tag-in/Tag-out (Physical information about patching)
- Status of all ports



IPADDRESS	ASSETNUM	FRAI	SLOT	PORT	NAME	STATUS	PORTTYPE	TAGIN	TAGOUT
10.140.56.74	DEVICE04267	1	3	1	Frame:1/Slot:3/Port:1	SPARE	ADSL	1/1	0/0
10.140.56.74	DEVICE04267	1	3	2	Frame:1/Slot:3/Port:2	BLOCKED	ADSL	1/2	0/0
10.140.56.74	DEVICE04267	1	3	3	Frame:1/Slot:3/Port:3	ISSUED	ADSL	1/3	0/0
10.140.56.74	DEVICE04267	1	3	4	Frame:1/Slot:3/Port:4	ISSUED	ADSL	1/4	0/0
10.140.56.74	DEVICE04267	1	3	5	Frame:1/Slot:3/Port:5	ISSUED	ADSL	1/5	0/0
10.140.56.74	DEVICE04267	1	3	6	Frame:1/Slot:3/Port:6	ISSUED	ADSL	1/6	0/0
10.140.56.74	DEVICE04267	1	3	7	Frame:1/Slot:3/Port:7	BLOCKED	ADSL	1/7	0/0

Figure.4.3: OSS sample port plan

The port plan is the first step for any new site, once the port plan is prepared and vetted, it is loaded to the inventory system. When the port plan is added to the inventory, the state of all ports are flagged as SPARE. The updated inventory is visible to exchanges on the basis of which the port allocation to a customer is carried out. If any port is assigned to the customer, its status is also updated in inventory and on the graphical interface which is being used for port assignment at exchange level. The provisioning system is capable of splitting one request into multiple tasks and then executing them on one or several network elements. Service provisioning information is used to get the card capacity, occupied ports per card and other state of ports.

4.2 RADIUS server Applied Model

The RADIUS servers used for the purpose of sending the accounting information to the external database. The RADIUS servers process all the incoming requests for the RADIUS clients referred to as BRAS in internet service provider network. AVP [16] and VSA [16] are treated to write the accounting information into the database. The Figure.4.4 explains the basic model for integration of RADIUS servers in a network and how the clients are connected to RADIUS server. The RADIUS server on the one side connects to the client and on the other side, it is connected to the external database. The request initiated by CPE reached BRAS through network element (DSLAM) and BRAS further distributes the requests on different RADIUS servers. The RADIUS servers process all the requests and records all logs in the external database.

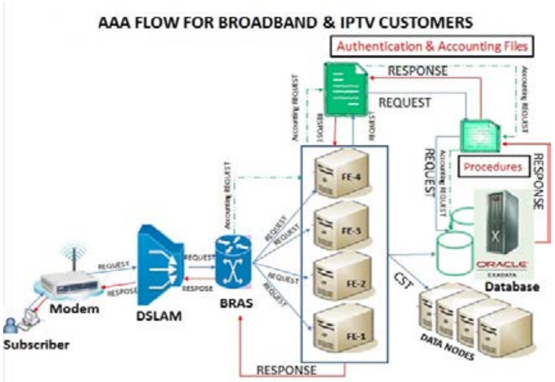


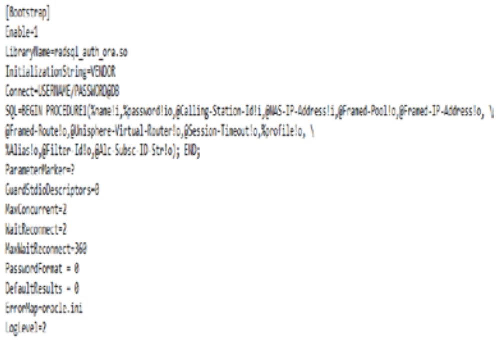
Figure.4.4: RADIUS connectivity diagram with external database

The method proposed here does not need any change or update to the standard network level configuration and architectural used for PPPOE based authentication. In mostly ISP the common protocol use at access side is PPP which is the same in my case. At customer side xDSL supported modems are used and they have direct connectivity to the BRAS using PPP. The PPP session remained established when CPI and BRAS are communicating on the basis of echo packets that are exchanged after some defined interval between both the devices. Usually, if within three minutes, echo packets are not received the established session cannot continue and is disconnected [1]. CPE is configured to send authentication credentials to the BRAS and BRAS asks the RADIUS server to authenticate user. The RADIUS server is configured for authentication, authorization and accounting (AAA) for all the incoming requests. The requests are further triggered to the external DB instead of generating any accounting on RADIUS servers. One of the important reasons external database is used is that if all types of accounting like (START, STOP and INTERIM) are enabled on the BRAS the processing of accounting on RADIUS server take more time and usually we run into space issues on the server whereas on external database there is no constraint with respect to space. Secondly, if any query is executed on external database it has zero impact on the RADIUS server.

The solution proposed by Zych [1] discussed two algorithms of thresholds, the first threshold is to determine the capacity of card which in our case is carried out by using information from the provisioning system whereas the second threshold is directly on the RADIUS server which in author opinion is not the preferred way when traffic load is high (millions of transactions per day) performing any filtering in raw accounting files of RADIUS servers (which are not indexed) usually take more time in extracting information and the output is very slow. The accounting sent to some external database is the preferred option. The output of searching any record from external database is 3 times faster than searching in the RADUIS server logs files. The BI system can also get the feed for RADIUS accounting from external database and correlate set of data obtained from different system to diagnose a problem and create incidents.

4.3 RADIUS Attributes used for classification

The incoming requests from BRAS generally known as Access-Request. The Access-Request contains several important attributes that are either attribute-value-pairs or vendor-specific-attributes as already discussed. The mapping of these attributes are carried out on the RADIUS server. The RADIUS server forwards the incoming requests toward the external database on which specific procedures resides. The RADIUS server established the connection with the external DB and triggers the procedure from its configuration script. The below Figure.4.5 shows a configuration file on a RADIUS server, when there is any incoming request on the RADIUS server from the BRAS and this file is called the RADIUS server connected the external database using connect parameter and runs a procedure in the external database (PROCEDURE1). The parameters of the incoming packets are passed to the external database through input parameters (%name!i) and output parameters (@Framed-Ip-Address!o) are received by RADIUS servers

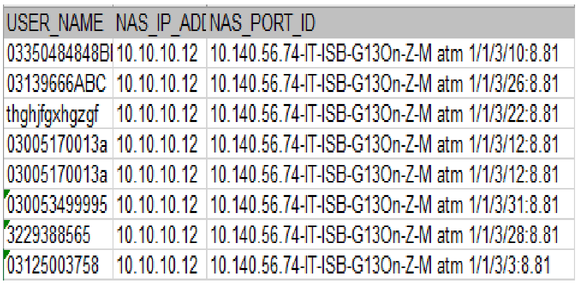


```
[Bootstrap]
Enable=1
LibraryName=radsql_auth_ora.so
InitializationString=VENDOR
Connect=USERNAME/PASSWORD@DB
SQL=BEGIN PROCEDURE1(%name!i,%password!io,@Calling-Station-Id!i,@NAS-IP-Address!i,@Framed-Pool!o,@Framed-IP-Address!o, \
@Framed-Route!o,@Unisphere-Virtual-Router!o,@Session-Timeout!o,%profile!o, \
%Alias!o,@Filter-Id!o,@Alc-Subsc-ID-Str!o); END;
ParameterMarker=?
GuardStdioDescriptors=0
MaxConcurrent=2
WaitReconnect=2
MaxWaitReconnect=360
PasswordFormat = 0
DefaultResults = 0
ErrorMap=oracle.ini
LogLevel=?
```

Figure.4.5: Sample file for connecting external database

4.4 Recording accounting in External Database

Similarly, the accounting information received from BRAS is directed to the external database using different attributes [16]. The proxy file on radius server is being used to map the incoming requests to different authentication and accounting methods. The accounting sent to the external database using RADIUS servers is of type START, STOP and INTERIM. Further, STOP accounting data is used for testing and stats gathering discussed below in result section. The accounting request initiated by BRAS is distinguished on the basis of value received in the attribute Acct-Status-Type [16]. When the value of this attribute is 2, it is considered as the stop of a running session is received and now the session disconnected. Such kind of incidents used to extract the results. There are also other important values received in other attributes on the basis of which filtering mechanism can be narrowed down and used in getting results. The information of the access device is received from BRAS in an attribute called Nas-Port-Id [16]. This attribute contains a string in which the unique IP-Address of each side is present and it also has the information about the frame, slot and port of each customer for which a PPPoE session was initiated.



USER_NAME	NAS_IP_ADI	NAS_PORT_ID
03350484848BI	10.10.10.12	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/3/10:8.81
03139666ABC	10.10.10.12	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/3/26:8.81
thghjfgxhgzgf	10.10.10.12	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/3/22:8.81
03005170013a	10.10.10.12	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/3/12:8.81
03005170013a	10.10.10.12	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/3/12:8.81
030053499995	10.10.10.12	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/3/31:8.81
3229388565	10.10.10.12	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/3/28:8.81
03125003758	10.10.10.12	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/3/3:8.81

Figure.4.6: RADIUS Accounting written to Database

The accounting information is continuously written to the database in different tables as per Figure.4.6. The integrated system processes the accounting information for the purpose of billing, offline analysis. The business intelligence system is included to analyze the data in real-time.

4.5 Inclusion of BI for real-time analysis

BI platform proposed is to forward the accounting information in real-time. It is capable to collect, integrate, analyze and present any raw data for the purpose of creating insight and useful real-time reporting on the basis of which action can be taken more efficiently. In the process of data analysis BI platform can discover useful information through structured or un-structured data. It can perform descriptive analytics, diagnostic analytics, predictive analytics or prescriptive analytics using the raw data as represented in Figure.4.7.

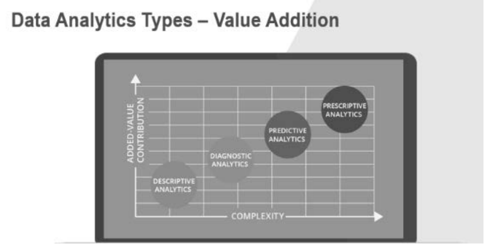


Figure.4.7: Type of analytics BI can perform

It may contain Ad-hoc query tool, Report writers, End-user applications, Modeling/mining tools and virtualization tool. The use of BI analytics enables an operator to view different reports on the dashboard. The reporting mechanism for an ISP is mentioned below.

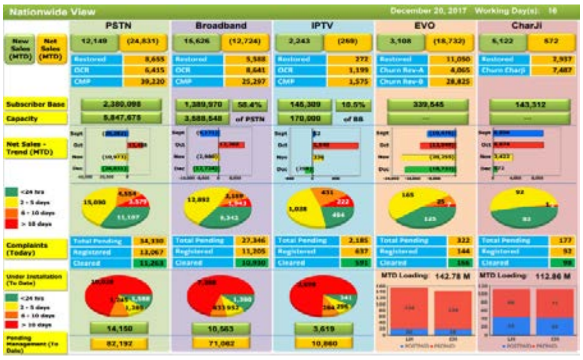


Figure.4-8: Sample dashboard report using BI for analytics

The Figure.4.8 shows sample dashboard report created using different dataset available in the BI system. The BI system gets data from different source systems and performs real time analysis through correlation of data sets to find out reasons to the problem and suggesting action need to addressed any issue.

4.6 Latest Techniques in Network Monitoring

According to author [22] to achieve productivity, better service quality based on QOS and high speed broadband services play vital role. Patterns and trends analysis of different service providers broadband speed were taken into consideration. TX and RX speed were recoded and analyzed. Software used for achieving this goal the author had used Solarwinds Orion product and using Matlab 2016a different tests were performed that included cumulative distribution and probability density function, variance monitoring tests, regression and correlation analysis and descriptive methods. The purpose was to figure out the optimal network latency for placement of high speed services in network. The extracted data is further organized and presented in the form of tables, charts and represented graphically.

SDN are globally adopted [23-26] and now a day work is being carried out for different type of networks like software defined network using big data analysis techniques.

Conventional network monitoring systems are not enough to meet data storing and real-time analytics requirement. Netflow based on big data as a monitoring object ensure four functions. Filebeat is used to collect Netflow and ensure reliable transfer of data in real-time on the basis of Logstash whereas the data is stored in ElasticSearch and data is analyzed and showed in real-time using Kabana. SDN enables separating control plan from the data plan by fixing the limitation within the current network. The intelligence is shifted to a controller which then copes with all different devices present in the data plan. Traffic engineering is used to monitor different network parameters. Monitoring of bandwidth is one of the important parameters among others. The counter maintenance is one of the key element for network devices and it is updated for every packet passing through the device like a switch and openFlow protocol was being used as it tracks record of different counters maintained within a specific device. Big data is real time monitoring technique which gathers the information about different counters and also has the capabilities for processing different counters. The proposed method focused on monitoring resources such as switch port, flow entries and flow tables and limited to layer two and layer three based monitoring. The security within a network is very essential for which solid approach is needed for access control and authenticating different devices. Whereas the scope of this research is to perform monitoring beyond layer two and layer three using Application layer protocol and also cater security features required for controlling any illegal access to resources.

Failure in a broadband network are keep on increasing [27] the author viewed areas where the probability of fault exists and had suggested an approach based on recursive neural network for long team and short term prediction. It was proposed that for telecom operator's inclusion of prediction methods is important for their strategy and management of proper network. The model proposed on the basis of neural network according to the author is prediction model that is well trained and data fed is appropriate, it supports in operation maintenance and proper workflow assignments. The factors taken into considerations with respect to network were NE outages, previous failures appeared in the network almost for one week and different network conditions such as weather conditions or network planned activities. Filtering of inaccurate data was also suggested before it was trained or used as input. Whereas, scope of this research is not limited to data sets available in the database but are used to perform analytics.

Conventional digital subscriber line (DSL) technologies are capable for high bandwidth for data communication and is broadly used. DSLAM have connection from many customers that are aggregated on single and high capacity connection [28-29]. Another author proposed a broadband diagnostics system that has the ability to gather information, store data and use historical data for comparison purpose to existing network elements [30]. It is limited to monitoring software based broadband at customer premises whereas proposed solution in this research is not limited to CPE as technique proposed here can monitor different issues that appears in the network.

There was another author [31] who unveiled methods for bandwidth related issues using network traffic monitoring and assessing load in the network, also reporting were carried out for utilized traffic and how the bandwidth can be reserved was also explored. The congestion in the network directly affect the performance and slow down processing. Quality of service is also one of the important parameter [32] considering private enterprise network and public broadband services. Different type of traffic requires different QoS and this traffic prioritization is important as some applications are bandwidth hungry and if

QoS is not implemented the desired performance cannot be achieved. Performance level are associated to required bit rate, network delays, jitter and packet drops as they are important parameters for an application to operate at desired level. Real time streaming like VOIP, online gaming and IPTV services are very sensitive to delays and required fixed bandwidth. For good performance in broadband network different protocols and services are offered which supports QoS. MPLS is one of the example which route data from one network node to another based on shortest path labels instead on adopting other paths [32]. The proposed model in this research work will not absolute the above monitoring technique but it may be helpful in finding out QoS against any single customer using accounting logs like interim update and through frequent disconnection.

There was another model proposed by author [33]. An alternative path used for fault rectification and diagnostics of customer premises equipment (CPE) when there is a physical breakdown of cable or electrical impairment in the broadband service or CPE is functioning abruptly and cases where CPE is not configured properly. The alternative communicate device is placed at customer premises that provides diagnostics and configuration information about the defected CPE like gateway issue, network at premises and broadband network elements status. The proposed solution requires additional devices to be placed at customer premises and address the issues specific to access side of the network whereas method or approach used in this work is not limited to access side. Using the applied algorithm and accounting statistics may help an operator to use different reports to check how long a user services are interrupted and which type of issue being faced at the customer end.

Recently cloud services are offered for enhancement of broadband experience. The broadband services being controlled using different approaches discussed by another author [34]. According to the author, the process contains gathering user’s behavior information, usage information and physical layer data linked to broadband. Further the collected information was analyzed so that if statistics are fine different services can be offered to the customer like service profile enhancement. The LAN and WAN performance statistics were not centrally investigated, the proposed method had not addressed the contextual information but helps in determining the bandwidth requirement of a customer. The solution suggested to place a downloadable agent inside LAN, this agent collects the information for cloud and further this data was sent using WAN services over cloud for further analysis. The higher throughput of broadband connection is linked to different broadband service offering like OTT (Over The Top). The proposed solution in this research work may also be used for bandwidth enhancement and offering new services to the customer on the basis of line quality analysis and stability checks. User’s having good line experience very less disconnection and high download rate based on subscribed package.

Based on broadband service usage [35] a solution was proposed. The purpose was to analyze LAN and WAN performance through a central location. The information can be topology, geographical, network usage package, network quality, throughput linked, and behavior of network usage. On the basis of loop length operators decide the service products for a customer, whereas this method is not recommended for manually and physical fixing services related issue. The expressions designate a SR for upgrade and downgrade approvals using current and historical services condition information. Network performance mention throughput

(TCP/UDP), jitters, connectivity status, error rates, power (transmit/receive) rate etc. Increasing above parameters enhance the efficiency of the communication systems. The applied method in this work is helpful in finding out the disconnections reasons for any user and may be used as method for offering different services to customers having stable connections and configured on high bandwidth packages and is an efficient way to enhance the revenue.

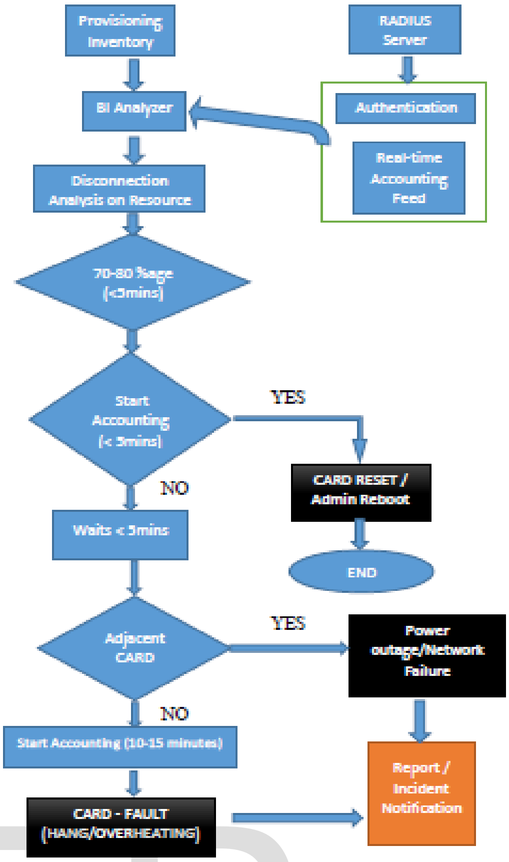
One similar research was carried out by author [36] on assigning initial profile to a CPE that is closed to the supported level (based on line, pair condition). Appling default profiles to new customers may resulted in frequent disconnection and instable services. A controlled look feedback mechanism basically is deployed in dynamic line management (DLM). In this process the profile applied on the line is based on the condition or according to scheduled operation criteria and operation of line is monitored time to time and based on that line rates are adjusted accordingly to avoid any frequent disconnections at customer end. The scheduled operation criteria are based on balancing stability of a connection through analyzed number of errors, reconnection behavior of a line, performance parameters analysis that is based on bandwidth, data rate and deleys. The modem is placed at the network side (i-e within aggregation device) DSLAM. At DSLAM signals from different modems are received and are multiplexed onto a single backhaul data connection to next aggregation point which may be some router/BRAS. DLM is one of the latest approach being deployed for monitoring the line quality and applying customized profiles to avoid any kind of disconnection but the approach discussed here in the research work may still be helpful in checking issues where resync frequency or disconnection is very high and on such cases changes are made on any new or old customer connection. Changing profile at access side also requires to implement and change package at AAA side, as both work at same time. If package at AAA is higher but profile is low the customer services will be restricted to less speed, similarly if profile is high at access side but package is low at AAA side customer will still face speed issues. In mostly networks profiles are pushed from AAA in response to ACCESS-REQUEST from BRASes.

In another model [37] author had proposed a method for monitoring and detecting fault between a device and broadband remote access server (BRAS). Statically significant samples of CPE of a S-VLAN were collected and monitored over a predetermined time period. Average number of CPE connected for each period was determined and connectivity model generated. Rules were imposed based on the variation in connectivity, if any fault situation was pointed out with the help of logical and physical topology of network fault location was found, based on it the rectification method was applied. The method discussed above can be one of the approach used for monitoring fault based on S-VLAN but on the other hand this approach may complex the monitoring and fault detection process due to lack of centralized database and historical information. The method discussed in this research work is more efficient in author opinion due to availability of historical and current data, also information of each site can be find using NAS-PORT-ID information available in the RADIUS request. In network mostly DSLAMs are configured to send circuit-id and option-82 information to AAA servers which may be used to find location from where user is sending the connection request.

4.7 Implementation

For the purpose of implementation, the enterprise provisioning system (OSS) is used. The purpose for which, this system is added to research work is to fetch the information of all network elements port plans. It enables me to get the exact capacity for number of cards installed, available slots, number of ports and status of the ports. A test RADIUS server is installed and configured as part of enterprise network. Then on the RADIUS server mapping is performed to send the requests from different vendors towards a specific configuration file. The configuration file being used contains the connection information for the external database. For connecting RADIUS server to the external database oracle client (OCI) is used. The configuration files on the RADIUS server are configured to call the procedures available on the external database. When authentication request reached the RADIUS server through the BRAS, RADIUS server configuration files are called to trigger procedures whereas when the accounting request is received, the configuration files for accounting on the RADIUS server insert the accounting data into the external database. The accounting data is used to extract the results for bulk disconnections on any specific card. The capabilities of BI analytics explored and made it part of applied design for avoiding any production load and performance issues on RADIUS servers and external database. The external database sends the accounting data to BI system through using scripts. The data is received by BI system in near to real-time. BI perform analytics on the data and can generate reports for respective teams. On the basis of those reports incidents can be created.

4.7.1 Applied Algorithm for detection of failures


Provisioning Inventory
RADIUS Server
BI Analyzer
Authentication
Real-time Accounting Feed
Disconnection Analysis on Resource
70-80 %age (<3mins)
Start Accounting (< 3mins)
YES
CARD RESET / Admin Reboot
NO
Waits < 3mins
END
Adjacent CARD
YES
Power outage/Network Failure
NO
Start Accounting (10-15 minutes)
Report / Incident Notification
CARD - FAULT (HANG/OVERHEATING)

The business analytics system used the inventory of provisioning system for the purpose of identification of network resource provisioned, total number of cards on which customers are provisioned, total capacity of card it is calculated on the basis of issued ports of the card in OSS, it may track record for the spare ports and blocked ports and update the data on the basis of any change or update in the provisioning inventory so that the provision inventory remained synched with the BI inventory. The information about the provisioned username on each port of the card of a resource can be obtained from provisioning system (subjected to the availability of information in provisioning system). In this algorithm the BI system takes the usernames information from the external database table. The authentication table tells about both the active username and inactive username (Inactive usernames are those that are temporary closed due to non-payment or any other reason). The preferred way is to get username status information too from the provisioning system. When provisioning is done through automation all updates to authentication tables of external databases are processed or triggered from the provision system. Once the request of provision system is completed successfully it updates the provisioning inventory with the latest state of the resource (for example if any user has to be suspended it is provisioning system that initiates the request and update the port status Blocked or Closed). When the username is suspended in the external database the provisioning system in parallel also deactivate the port on the resource for proper management and getting desired results for monitoring. This will also ensure that provisioning inventory remained in-sync with both the resource and database inventory. The algorithm applied will not perform any computation on the RADIUS servers because the logs files created on the servers are not structured (raw data). Searching from several thousands of rows from different RADIUS servers for a specific problem is not recommended way because there may be several RADIUS servers configured for authentication and accounting on the BRAS and the BRAS is sending requests to them in round-robin. This means that for a specific username the authentication request can land on any one of the RADIUS server whereas its START, STOP or INTERIM accounting will be processed too from different servers. Gathering information from different files against one PPPOE session is not possible. In such cases where several RADIUS servers are configured and traffic load is high (millions of transactions per day) the external databases (like ORACLE DB) is used and in that scenario all the RADIUS servers are configured to call authentication procedures that are created on the external database for PPPOE usernames authentication. Once a user is authenticated the accounting START, STOP or INTERIM is written to their respective tables in the DB. The data stored in the external database is properly indexed and the query response time is much faster than searching in RADIUS server's logs files. In high traffic scenario where update-on-interim is enabled the interim update time set on the BRAS is between 30mins to 1hr (frequent updates will populate the DB and may result in storage issues). The BI systems can be further integrated to the database servers for fetching the CDRs in real-time that can be further used by the BI system for analyzing purpose.

The BI system had complete updated information about all the resources in its inventory like the number of card installed on a specific resource, total number active customers on card, total number of subscribers sending interim updates. The analyzer updates the report for a specific resource after an hour on the bases of unique sessions Started, Stopped and ongoing sessions. When bulk disconnection is triggered on a card this information will be available in real-time both in the external database and BI system. Then BI analyzer will check from the stop accounting records that if 70-80% of sessions are disconnected within period less than five minutes during the time interval of 1hr. On confirmation that all users on the resource are disconnected it will further search in the start accounting logs for specific card and users to see if any start accounting for disconnected users or ports received within next 5mins or not (In case the card is rebooted / reset all the connected users on the card are reset and they will reconnect immediately). If no start accounting information is received within (5-10 minutes) against users or ports of the resource, then it will be further monitored. The algorithm will also check the status of ports or users connecting on the adjacent card to localize the issue (if this issue is on all the cards of the resource or only card specific). If the issue is not on the adjacent card, then it means that it is not a resource level issue. If no start accounting is received till the waiting time limit is reached (usually set to 10-15 minutes) the BI system will create an incident or generate an outage report i.e Card Down. It will keep on monitoring the problematic resource only till the maximum time is exceeded. The algorithm also helps operators to keep track on SLA (The time incident is created and till it is resolved). Due to non-availability of this kind of monitoring in an operator network the users suffers for several days and SLA breached (Cases discussed in Result Section Chapter 5).

RESULTS AND DISCUSSION

5.1 Generalize Model used for Monitoring Mass Failures

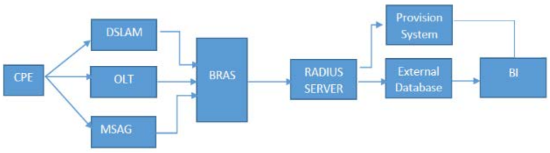
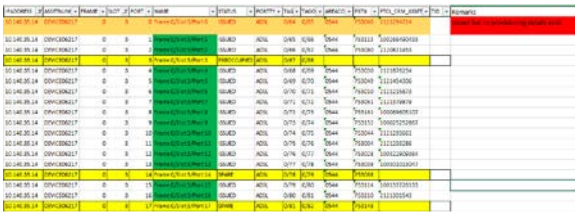


Figure.5.1: Model proposed for efficient monitoring

Provisioning system inventory is used to find out actual ports density for a specific card on which the fault has occurred. Using provisioning system, we can obtain exact information about ports that are issued to the customers and are in use. It also tells us about the ports which are not currently assigned to any user and currently in spare state. Some of the customers on the card are in blocked state. The reason for blocked ports may be due to non-payment, customer request or ports being declared as faulty (once ports declared as faulty no new customer can be provisioned on that specific port).

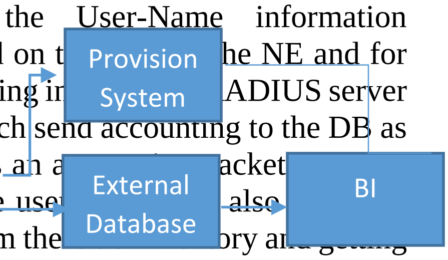


IPADDRESS	ASSETNAME	FRAME	SLOT	PORT	NAME	STATUS	PORTTYPE	TAG	TAGO	AREACODE	PSTN	PTCL_CRM_ASSET	TID	Remarks
10.140.35.14	[illegible]	0	3	0	Frame 0/Slot 3/Port 0	ISSUED	ADSL	0/64	0/65	0544	753040	[illegible]		[illegible]
10.140.35.14	[illegible]	0	3	1	Frame 0/Slot 3/Port 1	ISSUED	ADSL	0/65	0/66	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	2	Frame 0/Slot 3/Port 2	ISSUED	ADSL	0/66	0/67	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	3	Frame 0/Slot 3/Port 3	PREOCCUPIED	ADSL	0/67	0/68					
10.140.35.14	[illegible]	0	3	4	Frame 0/Slot 3/Port 4	ISSUED	ADSL	0/68	0/69	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	5	Frame 0/Slot 3/Port 5	ISSUED	ADSL	0/69	0/70	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	6	Frame 0/Slot 3/Port 6	ISSUED	ADSL	0/70	0/71	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	7	Frame 0/Slot 3/Port 7	ISSUED	ADSL	0/71	0/72	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	8	Frame 0/Slot 3/Port 8	ISSUED	ADSL	0/72	0/73	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	9	Frame 0/Slot 3/Port 9	ISSUED	ADSL	0/73	0/74	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	10	Frame 0/Slot 3/Port 10	ISSUED	ADSL	0/74	0/75	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	11	Frame 0/Slot 3/Port 11	ISSUED	ADSL	0/75	0/76	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	12	Frame 0/Slot 3/Port 12	ISSUED	ADSL	0/76	0/77	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	13	Frame 0/Slot 3/Port 13	ISSUED	ADSL	0/77	0/78	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	14	Frame 0/Slot 3/Port 14	SPARE	ADSL	0/78	0/79	0544	[illegible]			
10.140.35.14	[illegible]	0	3	15	Frame 0/Slot 3/Port 15	ISSUED	ADSL	0/79	0/80	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	16	Frame 0/Slot 3/Port 16	ISSUED	ADSL	0/80	0/81	0544	[illegible]	[illegible]		
10.140.35.14	[illegible]	0	3	17	Frame 0/Slot 3/Port 17	SPARE	ADSL	0/81	0/82	0544	[illegible]			

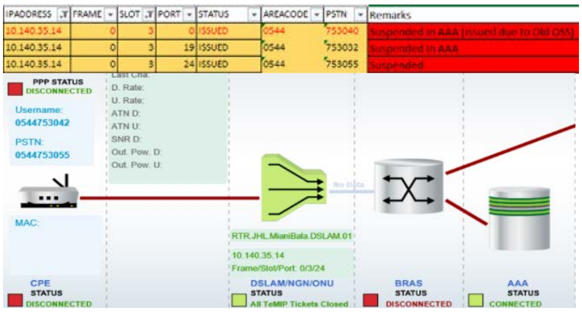
Figure.5.2: OSS port plan status information

In the Figure.5.2 Port plan for specific site is shown where FRAME correspond to physical shelf of the network element, SLOT give information about the number of cards installed and PORT column contains the information about the number of ports available on each card. This is actually third card of an NE having total ports capacity of 32 which means that on this card we can provide services to only 32 customers. Using the OSS inventory the information is extracted about the ports which are in service (out of 32 ports on 24 ports customers were provisioned). The other ports were either in blocked state or spared.

In this case AAA external database is used to fetch the User-Name information provisioned on t [illegible] he NE and for the accounting in [illegible] ADIUS server is used which send accounting to the DB as soon it gets an a [illegible] acket BRAS. The user [illegible] also fetched from the [illegible] ory and getting that from OSS inventory is more convenient than getting it from the DB. In our case, the AAA external DB is due to below mentioned reasons (some of the information can be obtained from OSS inventory subjected to the availability).



- If user is suspended due in non-payment the port status in OSS is reflected as Issued. It should be in blocked state till the user services are restored.
- Using port inventory information of OSS and correlating it with the information available in the AAA external DB it is easy to find out the which users are active and which are suspended.



IPADDRESS	FRAME	SLOT	PORT	STATUS	AREACODE	PSTN	Remarks
10.140.35.14	0	3	0	ISSUED	0544	753040	Suspended in AAA (issued due to Old OSS)
10.140.35.14	0	3	19	ISSUED	0544	753032	Suspended in AAA
10.140.35.14	0	3	24	ISSUED	0544	753055	Suspended

PPP STATUS
DISCONNECTED
Username:
0544753042
PSTN:
0544753055
MAC:
Last Cha:
D. Rate:
U. Rate:
ATN D:
ATN U:
SNR D:
Out. Pow. D:
Out. Pow. U:
RTR.JHL.MianiBala.DSLAM.01
10.140.35.14
Frame/Slot/Port: 0/3/24
CPE STATUS
DISCONNECTED
DSLAM/NGN/ONU STATUS
All TeMIP Tickets Closed
BRAS STATUS
DISCONNECTED
AAA STATUS
CONNECTED

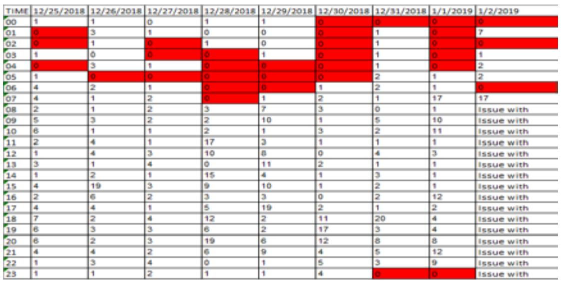
Figure.5.3: Connection status of suspended users

The Figure.5.3 shows the status against a username suspended in AAA but port inventory is showing issued. If a customer is deactivated in AAA, the port status should also need to be updated in OSS so that the capacity of card remained sync in BI and during finding out any fault on the card correct capacity of card can be calculated.

The BRAS sends requests to the RADIUS servers for validation of requests using User-Name, Password or any other attributes. As the RADIUS server receives thousands of requests (authentication, accounting) per second in our case the authentication requests are sent to external database for validation because they are highly capable to process bulk requests in parallel and more efficiently than RADIUS servers. The RADIUS server received the response from database in case of each request. On the basis of that response the RADIUS server either Accept or Reject the users. This response is also sent back to the BRAS which established the PPP session for the user. The BRAS sends the accounting messages to RADIUS server for each individual session established. The accounting messages sent by BRAS to RADIUS servers are distinguished on the bases of RADIUS attribute Acct-Status-Type value. The Acct-Status-Type value when equal to 1 indicates that this is an accounting Start message for the session. If it sends Acct-Status-Type value equals to 2, this means that the session has disconnected. Similarly, Acct-Status-Type value equals to 3 means that current session is in progress and customer is still connected but in this accounting message the value of resources used by the customers are updated. The Acct-Status-Type value equal to 3 is also known as Interim accounting. The interim accounting is triggered after a pre-defined interval set on the BRAS. In high traffic scenarios it is set to 30-minutes or 1-hour. In our case it is configured to 30- minutes.

Update-On-Interim may be enabled on the RADIUS server when BRAS is configured to send the interim updates so that the sessions are updated on RADIUS servers once the interim accounting is received through BRAS. When interim accounting is enabled and due to huge value of accounting logs it may be impossible to store logs on the RADIUS servers and any searching using these logs on RADIUS servers may results into performance issues. Due to this reason such logs are forwarded to the external database for easy process are avoid any performance problems.

Accounting data of RADIUS server is used that is sent to the external DB in real time for the purpose of gathering statistics about the network element on which card issue was observed. The stop accounting is used information to observe last 10-15days trends for customer on that card. It is observed that customer disconnection per hour is variable as discussed in the Figure.5.4 and when there is no disconnection during an hour it does not means that there is no customer connected on the card but this information is obtained from interim accounting.



TIME	12/25/2018	12/26/2018	12/27/2018	12/28/2018	12/29/2018	12/30/2018	12/31/2018	1/1/2019	1/2/2019
00	1	1	0	1	1	0	0	0	0
01	0	3	1	0	0	0	1	0	7
02	0	1	0	1	0	0	1	0	0
03	1	0	0	0	1	0	1	0	1
04	0	3	1	0	0	0	1	0	2
05	1	0	0	0	0	0	2	1	2
06	4	2	1	0	0	1	2	1	0
07	4	1	2	0	1	2	1	17	17
08	2	1	2	3	7	3	0	1	Issue with
09	5	3	2	2	10	1	5	10	Issue with
10	6	1	1	2	1	3	2	11	Issue with
11	2	4	1	17	3	1	1	1	Issue with
12	1	4	3	10	8	0	4	3	Issue with
13	3	1	4	0	11	2	1	1	Issue with
14	1	2	1	15	4	1	3	1	Issue with
15	4	19	3	9	10	1	2	1	Issue with
16	2	6	2	3	3	0	2	12	Issue with
17	4	4	1	5	19	2	1	2	Issue with
18	7	2	4	12	2	11	20	4	Issue with
19	6	3	3	6	2	17	3	4	Issue with
20	6	2	3	19	6	12	8	8	Issue with
21	4	4	2	6	9	4	5	12	Issue with
22	1	3	4	0	1	5	3	9	Issue with
23	1	1	2	1	1	4	0	0	Issue with

Figure.5.4: Everyday connectivity trend on a card

5.2 Limitations in previous works

The proposed solution by Zych [1] was based on variable thresholds related to the capacity of each card. As all the users may not be active on the card and threshold based on number of active users is very difficult to implement because this option requires searching the last interim update period at least 6hr or if no interim accounting, then it must cover the longest allowed duration of a PPP session (24h in most networks). Searching this in real time within the RADIUS server when transactions per day is very high it will generate high-load and is difficult to implement. It is further proposed by Zych [1] solution to such type of monitoring is to use hybrid of two thresholds. The first threshold fixed for the whole network to 30-40% of the capacity of smallest card in the network due to the reason capacity of card is not known and it will reduce the searching within the RADIUS logs for PPP sessions. Furthermore, it was suggested that instead of X% capacity of the smallest card it is better to find variable thresholds related to the card. This limitation is covered in my research work by efficiently finding the capacity of users on the card and setting the threshold accordingly.

5.3 Resolution to known limitations

In this research work prior limitation with respect to capacity of card is addressed. Now we know the capacity of card using both OSS and External DB. In second algorithm of hybrid threshold again the searching within the RADIUS history was proposed where the algorithm will check the more complex threshold of percentage of active PPP sessions on the resources. The active PPP session varies on the resource based on results gathers from external database against different cards. The card capacity is known in our case and statistics of data gathered from monitored resource indicates that applying both hybrid thresholds as proposed by Zych[1] may not point exactly to the problem. Some other approach is required to detect issues on card where active users on cards are less than 30-40%.

Let us consider the first threshold as proposed by Zych[1] which is fixed for the whole network and triggered when 30-40% of the capacity of smallest card is met. In network elements the smallest card is 16 ports and largest card may be up-to 64 or 74 ports. The cards are not fully occupied on the network element. In the case of only one user active on a card and if the card is hanged or become faulty due to some reason then the suggested first condition (first threshold) will never be satisfied, if the first threshold is not met, then the other threshold will also not be checked.

Keeping in view those limitations, it is very necessary to know the exact capacity of the card. Once the capacity of each resource is known the threshold can be implemented on the bases of issued ports on a specific card (other ports are still not allocated to any customer and are free in the system). The proposed solution here gives 100% of accuracy for finding the capacity of each card individually for any network element.

The daily trends observed for disconnection per hour on the specific card of the resource using the accounting information available in the external database. Important attributes received in the accounting messages are inserted in to specific tables of the external database. The attribute name and the type of values they can be contained are defined by RADIUS accounting RFC [16]. Initially, the Acct-Status-Type [16] attribute is used to filter the data for stop accounting. On the bases of stop accounting the daily trends for users on the problematic card is analyzed.

The card occupancy which is obtained from OSS and External DB showed that out of 32 ports on the problematic card 24 ports are in use. Then the data from the accounting records available in the external database is extracted to verify the number of distinct ports that are sending accounting information. The last eleven day’s data showed that the maximum record ports are below the number of active ports in the OSS (The maximum number of ports recorded equals 21). The card capacity is easily known using the co-relation of OSS and External DB (Other ports are issued in OSS but customers are suspended on these ports due to non-payment/ any other reason).

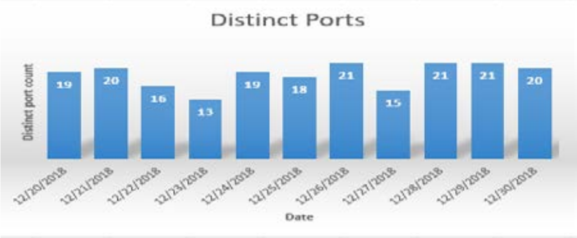


Figure.5.5: Distinct ports trends on a card

Further the trends for user's disconnection per hour is analyzed (before and after the incident).

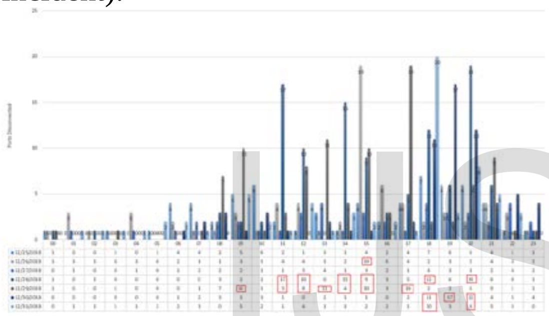
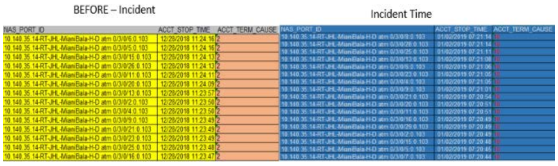


Figure.5.6: High disconnection of ports on a card

The data sets obtained in Figure.5.6 for high disconnections within a minute or two was checked from last hour accounting data. It was observed that two prominent reasons due to which customer sessions were disconnected were Lost-Carrier and NAS-Request. Before the incident around 14 distinct ports were disconnected in 1-2minutes and in that specific case the recorded cause code was Lost-Carrier. Whereas at the incident when card become faulty around 17 distinct users were disconnected and in this case the cause code recorded is NAS-Request referred to Figure.5.7. After the incident there were no stop accounting not even from a single user running on this card, which indicates towards an issue or problem with the card.



BEFORE – Incident

NAS_PORT_ID	ACCT_STOP_TIME	ACCT_TERM_CAUSE
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/6:0.103	12/28/2018 11:24:16	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/5:0.103	12/28/2018 11:24:16	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/15:0.103	12/28/2018 11:24:13	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/26:0.103	12/28/2018 11:24:13	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/11:0.103	12/28/2018 11:24:11	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/20:0.103	12/28/2018 11:24:09	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/13:0.103	12/28/2018 11:23:57	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/2:0.103	12/28/2018 11:23:50	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/4:0.103	12/28/2018 11:23:50	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/9:0.103	12/28/2018 11:23:49	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/21:0.103	12/28/2018 11:23:49	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/23:0.103	12/28/2018 11:23:49	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/25:0.103	12/28/2018 11:23:48	2
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/16:0.103	12/28/2018 11:23:47	2

Incident Time

NAS_PORT_ID	ACCT_STOP_TIME	ACCT_TERM_CAUSE
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/8:0.103	01/02/2019 07:21:14	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/26:0.103	01/02/2019 07:21:14	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/25:0.103	01/02/2019 07:21:11	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/13:0.103	01/02/2019 07:21:08	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/6:0.103	01/02/2019 07:21:06	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/23:0.103	01/02/2019 07:21:05	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/4:0.103	01/02/2019 07:21:05	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/9:0.103	01/02/2019 07:21:01	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/21:0.103	01/02/2019 07:20:54	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/20:0.103	01/02/2019 07:20:51	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/11:0.103	01/02/2019 07:20:51	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/16:0.103	01/02/2019 07:20:49	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/29:0.103	01/02/2019 07:20:49	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/2:0.103	01/02/2019 07:20:49	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/15:0.103	01/02/2019 07:20:48	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/5:0.103	01/02/2019 07:20:45	[illegible]
10.140.35.14-RT-JHL-MianiBala-H-D atm 0/3/0/7:0.103	01/02/2019 07:20:44	[illegible]

Figure.5.7: Comparison of connected ports before and after incident

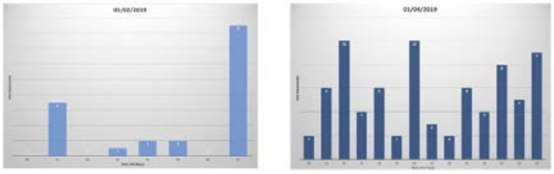
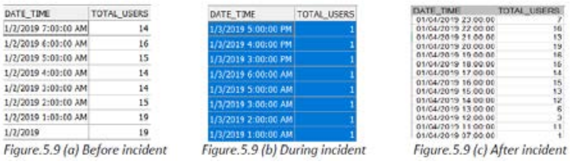


Figure.5.8: Long duration incident (greater than one day)

The Figure.5.8 shows the that the fault on the card lasted for more than one day. There was no accounting stop message for 3rd January,2019. The last accounting stop messages were recorded between 7am-8am on 2nd January. The issue was resolved at 9am on 4th January. During this duration the customers on faulty cards were unable to authenticate. If a proper mechanism was in placed, it would be resolved with in SLA duration (4-6hr).

The accounting information recorded in external database is used to extract information about the daily trend of interim accounting before the incident and at the time of the incident.



DATE_TIME	TOTAL_USERS
1/2/2019 7:00:00 AM	14
1/2/2019 6:00:00 AM	16
1/2/2019 5:00:00 AM	15
1/2/2019 4:00:00 AM	14
1/2/2019 3:00:00 AM	14
1/2/2019 2:00:00 AM	15
1/2/2019 1:00:00 AM	19
1/2/2019	19

Figure.5.9 (a) Before incident

DATE_TIME	TOTAL_USERS
1/3/2019 5:00:00 PM	1
1/3/2019 4:00:00 PM	1
1/3/2019 3:00:00 PM	1
1/3/2019 6:00:00 AM	1
1/3/2019 5:00:00 AM	1
1/3/2019 3:00:00 AM	1
1/3/2019 2:00:00 AM	1
1/3/2019 1:00:00 AM	1

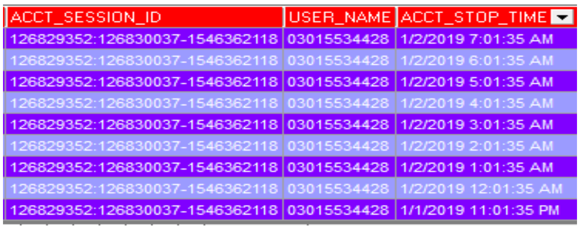
Figure.5.9 (b) During incident

DATE_TIME	TOTAL_USERS
01/04/2019 23:00:00	7
01/04/2019 22:00:00	16
01/04/2019 21:00:00	13
01/04/2019 20:00:00	19
01/04/2019 19:00:00	16
01/04/2019 18:00:00	16
01/04/2019 17:00:00	14
01/04/2019 16:00:00	15
01/04/2019 15:00:00	13
01/04/2019 14:00:00	12
01/04/2019 13:00:00	6
01/04/2019 12:00:00	3
01/04/2019 11:00:00	11
01/04/2019 07:00:00	1

Figure.5.9 (c) After incident

Figure.5.9 (a, b, c): Interim accounting per hour during and after the incident

The Figure.5.9(a) give information about the trends of interim accounting records for connected users on the card on 2nd January before the card became faulty. All the connected users were disconnected and their services were interrupted. From deep analysis of user data available in the database it was found that one user for which accounting was recorded in interim accounting table was actually a shifted case to another card due to which the accounting for only one user was recorded in interim accounting Figure.5.9(b). This case will not appear in the search if the ports information is recorded in the interim accounting.

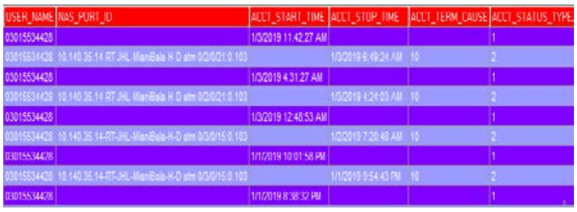


ACCT_SESSION_ID	USER_NAME	ACCT_STOP_TIME
126829352:126830037-1546362118	03015534428	1/2/2019 7:01:35 AM
126829352:126830037-1546362118	03015534428	1/2/2019 6:01:35 AM
126829352:126830037-1546362118	03015534428	1/2/2019 5:01:35 AM
126829352:126830037-1546362118	03015534428	1/2/2019 4:01:35 AM
126829352:126830037-1546362118	03015534428	1/2/2019 3:01:35 AM
126829352:126830037-1546362118	03015534428	1/2/2019 2:01:35 AM
126829352:126830037-1546362118	03015534428	1/2/2019 1:01:35 AM
126829352:126830037-1546362118	03015534428	1/2/2019 12:01:35 AM
126829352:126830037-1546362118	03015534428	1/1/2019 11:01:35 PM

Figure.5.10: Interim accounting record for user before incident

The Figure.5.10 is the last interim update for the user for which accounting was coming after the whole card was failed (usually not happen if filtering criteria is set to consider port). This also indicates the user last interim update for already connected session was updated at 7am (before the incident). At the time of incident this user services were affected too.

The Figure.5.11 give information about the start and stop time for user sessions and also update about the port used during the session.



USER_NAME	NAS_PORT_ID	ACCT_START_TIME	ACCT_STOP_TIME	ACCT_TERM_CAUSE	ACCT_STATUS_TYPE
03015534428		1/3/2019 11.42.27 AM			1
03015534428	10.140.35.14 RT JHL ManBala H-D atm 0/2/0/21:0.103		1/3/2019 6:49:24 AM	10	2
03015534428		1/3/2019 4.31.27 AM			1
03015534428	10.140.35.14 RT JHL ManBala H D atm 0/2/0/21:0.103		1/3/2019 4:24:03 AM	10	2
03015534428		1/3/2019 12:48:53 AM			1
03015534428	10.140.35.14-RT-JHL-ManBala-H-D atm 0/3/0/15:0.103		1/2/2019 7:20:48 AM	10	2
03015534428		1/1/2019 10:01:58 PM			1
03015534428	10.140.35.14-RT-JHL-ManBala-H-D atm 0/3/0/15:0.103		1/1/2019 9:54:43 PM	10	2
03015534428		1/1/2019 8:38:32 PM			1

Figure.5.11: Start and stop accounting for user (services shifted to another card)

The user was disconnected at 7:20am and was not able to authenticate for around 14hrs. The services of this user was shifted to another adjacent card for restoration of the services for this specific user but other users on the faulty card were not restored as they suffered till the card problem is attended. In the case of bulk disconnection at card level the proposed solution in this research work can efficiently trace the issue using accounting records of external database.

Similarly, the card faulty issue which took almost 10hrs in restoration. The trends of distinct ports disconnected per day is represented by Figure.5.12

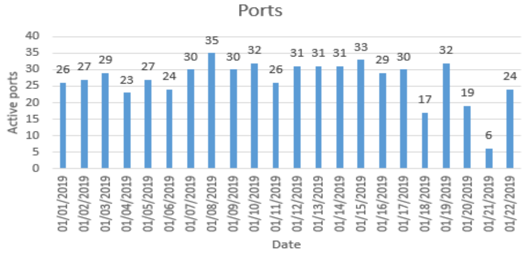


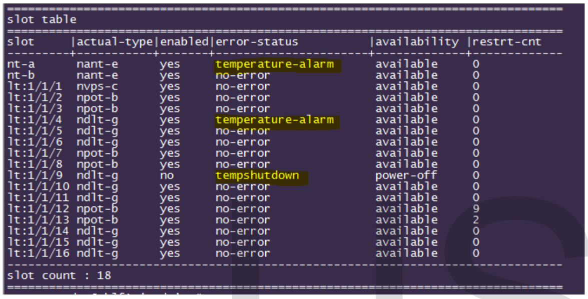
Figure.5.12: Decline in the port disconnection

It can be seen that on 21st January the count is very less as compared to previous trends. The trend is analyzed and it is observed that there were no accounting stop messages for users connecting to this cards onwards 4:30pm on 20th January. The accounting started at around 4am on 21st January which points towards an issue on the card. The restoration of this issue also takes more time than the expected time of recovery. During this duration, all customers trying to avail the service suffered. Sometime such kind of issues are too not noticeable by the customer until they prolong to several days (like the one explained in previous case).

The solution to this problem in author opinion is enable all types of accounting on the RADIUS servers and sent accounting information in real time to the external database and Business intelligence system as searching from the raw logs of RADIUS server is not recommended as it creates load on the severs when there are millions of transactions per day. The External database is excellent source for stats gathering and querying from historical data. Similarly, the BI platform takes the data from external databases in real time, do correlation based on historical and real-time data.

5.4 Over-heating of card issue detection:

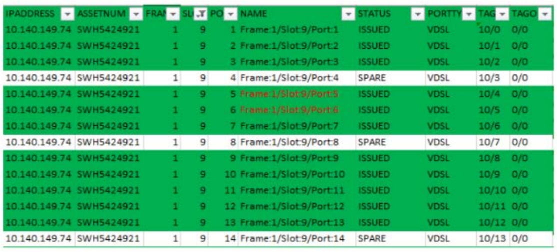
In different kinds of vendor devices, the behavior of subscribers running on the problematic card is different. In the case of Huawei/Alcatel due to raise in the temperature within the network element ports of card got shutdown and due to this reason all connected users on the card are immediately disconnected. Similarly, the behavior of ZTE cards are different where connected users faced frequent disconnections due to high temperature threshold. If this issue is not noticed, the subscribers keep on suffering for long duration or until the temperature comes to normal range.



```
================================================================================
slot table
================================================================================
slot      |actual-type|enabled|error-status              |availability |restrt-cnt
----------+-----------+-------+--------------------------+-------------+-----------
nt-a       nant-e       yes     temperature-alarm          available     0
nt-b       nant-e       yes     no-error                   available     0
lt:1/1/1   nvps-c       yes     no-error                   available     0
lt:1/1/2   npot-b       yes     no-error                   available     0
lt:1/1/3   npot-b       yes     no-error                   available     0
lt:1/1/4   ndlt-g       yes     temperature-alarm          available     0
lt:1/1/5   ndlt-g       yes     no-error                   available     0
lt:1/1/6   ndlt-g       yes     no-error                   available     0
lt:1/1/7   npot-b       yes     no-error                   available     0
lt:1/1/8   npot-b       yes     no-error                   available     0
lt:1/1/9   ndlt-g       no      tempshutdown               power-off     0
lt:1/1/10 ndlt-g        yes     no-error                   available     0
lt:1/1/11 ndlt-g        yes     no-error                   available     0
lt:1/1/12 npot-b        yes     no-error                   available     9
lt:1/1/13 npot-b        yes     no-error                   available     2
lt:1/1/14 ndlt-g        yes     no-error                   available     0
lt:1/1/15 ndlt-g        yes     no-error                   available     0
lt:1/1/16 ndlt-g        yes     no-error                   available     0
--------------------------------------------------------------------------------
slot count : 18
================================================================================
```

Figure.5.13: Status of cards on A DSLAM

The 9th card total capacity is obtained from the OSS provisioning system. The total ports on the 9th card were 48-ports out of which 29 ports were issued. The external database used to first find out the User-Name associated each provisioned port of this card.



IPADDRESS	ASSETNUM	FRA	SL	PO	NAME	STATUS	PORTTY	TAG	TAGO
10.140.149.74	SWH5424921	1	9	1	Frame:1/Slot:9/Port:1	ISSUED	VDSL	10/0	0/0
10.140.149.74	SWH5424921	1	9	2	Frame:1/Slot:9/Port:2	ISSUED	VDSL	10/1	0/0
10.140.149.74	SWH5424921	1	9	3	Frame:1/Slot:9/Port:3	ISSUED	VDSL	10/2	0/0
10.140.149.74	SWH5424921	1	9	4	Frame:1/Slot:9/Port:4	SPARE	VDSL	10/3	0/0
10.140.149.74	SWH5424921	1	9	5	Frame:1/Slot:9/Port:5	ISSUED	VDSL	10/4	0/0
10.140.149.74	SWH5424921	1	9	6	Frame:1/Slot:9/Port:6	ISSUED	VDSL	10/5	0/0
10.140.149.74	SWH5424921	1	9	7	Frame:1/Slot:9/Port:7	ISSUED	VDSL	10/6	0/0
10.140.149.74	SWH5424921	1	9	8	Frame:1/Slot:9/Port:8	SPARE	VDSL	10/7	0/0
10.140.149.74	SWH5424921	1	9	9	Frame:1/Slot:9/Port:9	ISSUED	VDSL	10/8	0/0
10.140.149.74	SWH5424921	1	9	10	Frame:1/Slot:9/Port:10	ISSUED	VDSL	10/9	0/0
10.140.149.74	SWH5424921	1	9	11	Frame:1/Slot:9/Port:11	ISSUED	VDSL	10/10	0/0
10.140.149.74	SWH5424921	1	9	12	Frame:1/Slot:9/Port:12	ISSUED	VDSL	10/11	0/0
10.140.149.74	SWH5424921	1	9	13	Frame:1/Slot:9/Port:13	ISSUED	VDSL	10/12	0/0
10.140.149.74	SWH5424921	1	9	14	Frame:1/Slot:9/Port:14	SPARE	VDSL	10/13	0/0

Figure.5.14: Card capacity estimation using OSS information

The User-Name information stored in external database gives the exact picture about the total number of users active for this card and users that are suspended or temporary closed. It is found that out of 29 ports issued through OSS the active users were 25 in the database while other 4 users were in suspended state. This means that from the suspended port no requests will be entertained by AAA server during the phase of authentication and there will be no accounting too if used requests failed at the time of authentication request. The best approach is to update the status of ports in OSS liked instead of showing them as issued it should be something like blocked/temporary closed.

Once active user's information is available, the accounting trends based on the ports and usernames on the external database using different SQL queries is observed. From reviewing the logs, it was noticed that there was no accounting record in database against subscribers provisioned on that card on 30th January 2019 between 10:34am till 13:17pm. The outage recorded is between 2-3hrs and during this outage all the customers were unable to avail any kind of services. The disconnection trends for last 10 days is also discussed in Figure.5.15

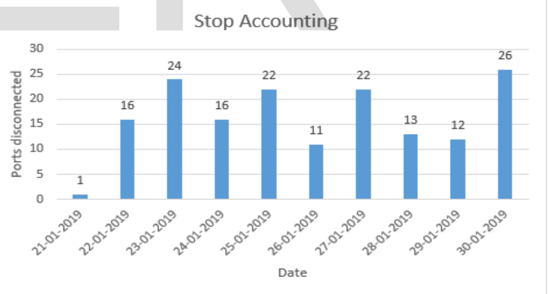


Figure.5.15: Last 10-days disconnection trends

The low disconnection does not indicate that total number of connected users on the card. To obtain all the users against the allocated ports of OSS accounting tables information of database is analyzed. From accounting start/stop records the users can be fetched easily (if username information is not available in OSS but the best option is to have this information too in OSS). Furthermore, these users are used to filter and see the behavior of interim accounting per day against them. It is evident from the trends that where the disconnections (as shown in Figure.5.15) is low per day there are other users of same card connected during the same time and availing the services without any interruption. The interim accounting trends per hour on 21st January (where only one distinct user was disconnected) is discussed in Figure.5.16.

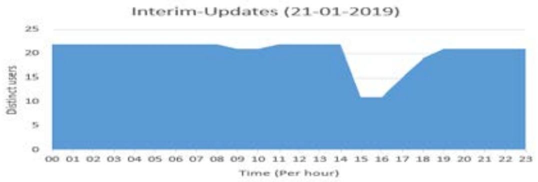


Figure.5.16: Interim accounting on a card for whole day

The above figure indicates that they are continuously availing the services and are sending interim updates (set to 30mins or 1hr where traffic load is high) after a predefined time period.

Further it is observed that interim accounting based analysis directly on radius servers required additional resources and is not the recommended way of searching data from millions of records. In the external database the data is available in real time and properly indexed. This enhances the capabilities for searching and every query is answered within few seconds.

A query based on searching for User-Name [2] available (correlation of OSS/DB data) from the interim accounting table. Due to huge number of entries in the table the total time taken to complete the search was less than 25 minutes.

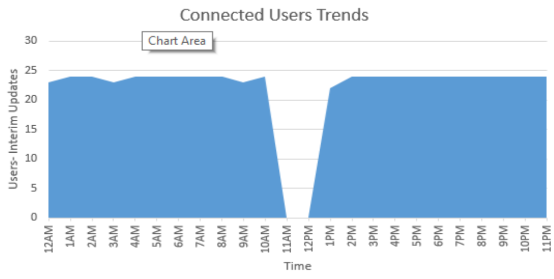
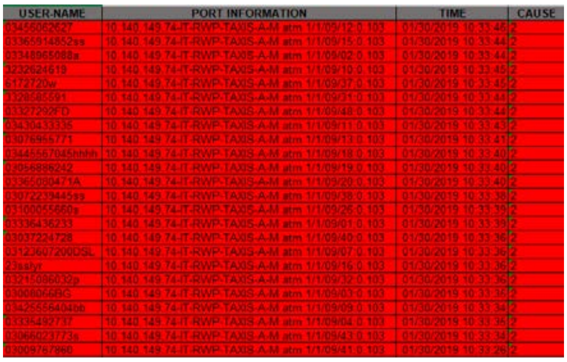


Figure.5.17: Incident where interim accounting stopped for users

The above figure.5.17 clearly indicates that during the overheating period all the connected users got disconnected and no interim accounting even for a single user on this card is received this surely indicates a fault situation for this card. Once the issue was resolved the trends become normal.

5.5 Bulk Disconnection Detection



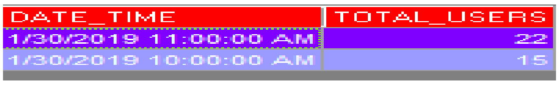
USER-NAME	PORT INFORMATION	TIME	CAUSE
03455062627	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/12:0.103	01/30/2019 10:33:46	2
03365914852ss	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/15:0.103	01/30/2019 10:33:44	2
03348965088a	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/02:0.103	01/30/2019 10:33:44	2
3232624619	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/10:0.103	01/30/2019 10:33:45	2
6172720w	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/37:0.103	01/30/2019 10:33:45	2
3328585591	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/31:0.103	01/30/2019 10:33:44	2
03327292FD	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/48:0.103	01/30/2019 10:33:44	2
03430433335	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/11:0.103	01/30/2019 10:33:43	2
03076965771	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/13:0.103	01/30/2019 10:33:41	2
03445567045hhhh	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/18:0.103	01/30/2019 10:33:40	2
03056886242	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/19:0.103	01/30/2019 10:33:40	2
03365080471A	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/20:0.103	01/30/2019 10:33:40	2
03072239445ss	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/38:0.103	01/30/2019 10:33:38	2
03100055660s	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/26:0.103	01/30/2019 10:33:39	2
03336436233	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/01:0.103	01/30/2019 10:33:39	2
03037224728	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/40:0.103	01/30/2019 10:33:36	2
03123607200DSL	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/07:0.103	01/30/2019 10:33:36	2
23aslyr	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/16:0.103	01/30/2019 10:33:36	2
03215086032p	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/32:0.103	01/30/2019 10:33:36	2
03008066BG	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/03:0.103	01/30/2019 10:33:35	2
03425556404bb	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/09:0.103	01/30/2019 10:33:34	2
03335492737	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/04:0.103	01/30/2019 10:33:35	2
03066023773s	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/43:0.103	01/30/2019 10:33:34	2
03009767860	10.140.149.74-IT-RWP-TAXIS-A-M atm 1/1/09/41:0.103	01/30/2019 10:33:26	2

Figure.5.18: Bulk disconnection within 1-2 minutes

It is observed that with in one minute around 24 distinct users on one card were disconnected. The capacity of card is known and as per the card capacity 90% users were disconnected (29 provisioned users – 4 suspended users in database and total 25 active users on a card). When the users are disconnected this information is reflected immediately in the external database as RADIUS sever is sending accounting information to external database. When correct capacity of card is known any 30-40% threshold as proposed by Zych [1] can be applied for triggering algorithm. I have achieved almost 100% results by using the interim accounting data.

I have done a correlation based on the previous hour interim accounting information and current disconnections. The previous hour interim accounting gave me information about the total number of connected users on the card before the incident. Once the incident is triggered the total number of disconnected users (1-2mins) are compared to the value of interim accounting to get the exact percentage of users suffered. In this case there were 24 distinct users interim record in previous hour. There were also 24 users disconnected within a minute (100% disconnection).

Once this situation has appeared the algorithm is triggered and it will initially check for the interim accounting record within the same time period for the adjacent card to ensure that if it is any power outage or anything specific happened to the card.



DATE_TIME	TOTAL_USERS
1/30/2019 11:00:00 AM	22
1/30/2019 10:00:00 AM	15

Figure.5.19: Status of Interim accounting during incident time on adjacent card

The algorithm has detected that with in the same duration the interim accounting is recorded from same network element but the card from the different card. This points out an issue locally to the card instead of the whole NE. The algorithm further will check if the users disconnected on the cards are due to card reset or any other reason. In the case of card reset usually all the connected users on the card got disconnected immediately and accounting logs are recorded in the external database as bulk disconnection triggering on such incidents are not required if the disconnecting behavior is not repetitive (some time NOC persons performs manually operation on the card to reset or refresh services). In my case, the algorithm will further check for accounting start in external database for the affected users. If no accounting start is received within 10minutes, it will create an incident for the operation team to check the card. After every 10minutes it will check the accounting data only for specific users (This checking can also be based on card based but in my case in accounting start port information is not recorded in the external database). The best way to carry out this monitoring is through the BI platform. The BI get useful information from the OSS and External database. The information stored in external database is sent to BI in real time. The BI carry out the analysis create reports and dispatch incidents.

This approach is every effective in finding out issues that are not acknowledge or monitored at a central point. Using this approach, not only card capacity limitation is addressed but also finds out a way of monitoring more failures from a centralize location than any specific monitoring solutions available in the market.

5.6 CARD Reboot/ CARD Restart Incident Tracking

Incidents like card reboot and card reset are not a problem if they are not frequent. There are several reasons due to which card reboot or card reset occurs. The reason could be due to manually reset by operational staff, high temperature, physical removing card or any other reason. There is a problem if a card is reset several time it may drops all the customer once it is reset or due to frequent reset the card may become faulty. Once the card is reset all the connected customers disconnected immediately and try to reconnect again once the card is back to its normal state. The monitoring solution suggested here can find out card reset problems and further using the analytic system based on historic and present trends frequent disconnection on the card can be detected. The Figure.5.20 shows disconnected trends per hour on one of the card. During two incidents there were maximum users disconnected.

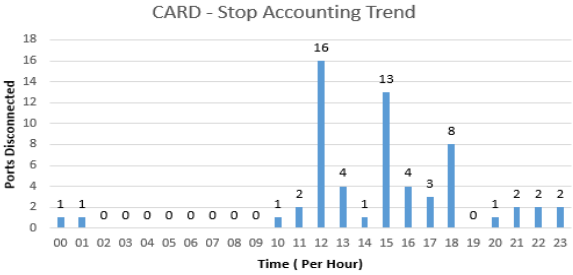
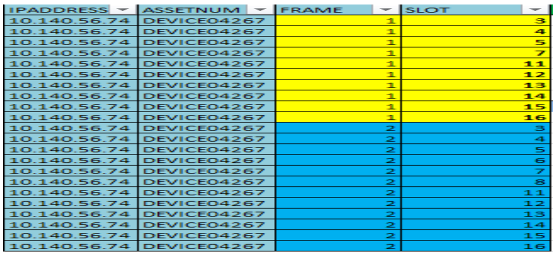


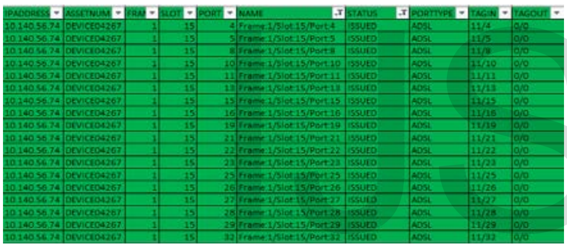
Figure.5.20: Disconnected users on a card (Per hour)



IPADDRESS	ASSETNUM	FRAME	SLOT
10.140.56.74	DEVICE04267	1	3
10.140.56.74	DEVICE04267	1	4
10.140.56.74	DEVICE04267	1	5
10.140.56.74	DEVICE04267	1	7
10.140.56.74	DEVICE04267	1	11
10.140.56.74	DEVICE04267	1	12
10.140.56.74	DEVICE04267	1	13
10.140.56.74	DEVICE04267	1	14
10.140.56.74	DEVICE04267	1	15
10.140.56.74	DEVICE04267	1	16
10.140.56.74	DEVICE04267	2	3
10.140.56.74	DEVICE04267	2	4
10.140.56.74	DEVICE04267	2	5
10.140.56.74	DEVICE04267	2	6
10.140.56.74	DEVICE04267	2	7
10.140.56.74	DEVICE04267	2	8
10.140.56.74	DEVICE04267	2	11
10.140.56.74	DEVICE04267	2	12
10.140.56.74	DEVICE04267	2	13
10.140.56.74	DEVICE04267	2	14
10.140.56.74	DEVICE04267	2	15
10.140.56.74	DEVICE04267	2	16

Figure.5.21: Total number of cards and frame uploaded in OSS

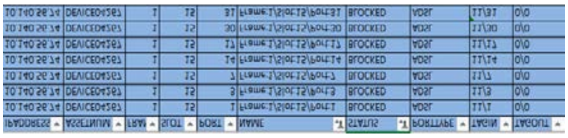
Whereas the Figure.5.21 is the information extracted for a complete resource. It gives information about the total number of cards installed on an NE. The Figure.5.22 below gives the capacity of card. The total card capacity of 15th card is 32 ports but all of the ports are not provisioned. Through provisioning data, the exact card capacity is obtained to know used ports. There are 18 ports currently in use, 7 ports in blocked state and 7 ports are in spare state.



IPADDRESS	ASSETNUM	FRAM	SLOT	PORT	NAME	STATUS	PORTTYPE	TAGIN	TAGOUT
10.140.56.74	DEVICE04267	1	15	4	Frame:1/Slot:15/Port:4	ISSUED	ADSL	11/4	0/0
10.140.56.74	DEVICE04267	1	15	5	Frame:1/Slot:15/Port:5	ISSUED	ADSL	11/5	0/0
10.140.56.74	DEVICE04267	1	15	8	Frame:1/Slot:15/Port:8	ISSUED	ADSL	11/8	0/0
10.140.56.74	DEVICE04267	1	15	10	Frame:1/Slot:15/Port:10	ISSUED	ADSL	11/10	0/0
10.140.56.74	DEVICE04267	1	15	11	Frame:1/Slot:15/Port:11	ISSUED	ADSL	11/11	0/0
10.140.56.74	DEVICE04267	1	15	13	Frame:1/Slot:15/Port:13	ISSUED	ADSL	11/13	0/0
10.140.56.74	DEVICE04267	1	15	15	Frame:1/Slot:15/Port:15	ISSUED	ADSL	11/15	0/0
10.140.56.74	DEVICE04267	1	15	16	Frame:1/Slot:15/Port:16	ISSUED	ADSL	11/16	0/0
10.140.56.74	DEVICE04267	1	15	19	Frame:1/Slot:15/Port:19	ISSUED	ADSL	11/19	0/0
10.140.56.74	DEVICE04267	1	15	21	Frame:1/Slot:15/Port:21	ISSUED	ADSL	11/21	0/0
10.140.56.74	DEVICE04267	1	15	22	Frame:1/Slot:15/Port:22	ISSUED	ADSL	11/22	0/0
10.140.56.74	DEVICE04267	1	15	23	Frame:1/Slot:15/Port:23	ISSUED	ADSL	11/23	0/0
10.140.56.74	DEVICE04267	1	15	25	Frame:1/Slot:15/Port:25	ISSUED	ADSL	11/25	0/0
10.140.56.74	DEVICE04267	1	15	26	Frame:1/Slot:15/Port:26	ISSUED	ADSL	11/26	0/0
10.140.56.74	DEVICE04267	1	15	27	Frame:1/Slot:15/Port:27	ISSUED	ADSL	11/27	0/0
10.140.56.74	DEVICE04267	1	15	28	Frame:1/Slot:15/Port:28	ISSUED	ADSL	11/28	0/0
10.140.56.74	DEVICE04267	1	15	29	Frame:1/Slot:15/Port:29	ISSUED	ADSL	11/29	0/0
10.140.56.74	DEVICE04267	1	15	32	Frame:1/Slot:15/Port:32	ISSUED	ADSL	11/32	0/0

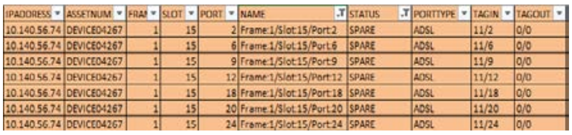
Figure.5.22: Port issued for a card in OSS

The Figure.5.23 shows total number of ports in block state for 15th card of a network resource under monitoring and Figure.5.24 gives total number of ports that are spare.



IPADDRESS	ASSETNUM	FRAM	SLOT	PORT	NAME	STATUS	PORTTYPE	TAGIN	TAGOUT
10.140.56.74	DEVICE04267	1	15	31	Frame:1/Slot:15/Port:31	BLOCKED	ADSL	11/31	0/0
10.140.56.74	DEVICE04267	1	15	30	Frame:1/Slot:15/Port:30	BLOCKED	ADSL	11/30	0/0
10.140.56.74	DEVICE04267	1	15	17	Frame:1/Slot:15/Port:17	BLOCKED	ADSL	11/17	0/0
10.140.56.74	DEVICE04267	1	15	14	Frame:1/Slot:15/Port:14	BLOCKED	ADSL	11/14	0/0
10.140.56.74	DEVICE04267	1	15	7	Frame:1/Slot:15/Port:7	BLOCKED	ADSL	11/7	0/0
10.140.56.74	DEVICE04267	1	15	3	Frame:1/Slot:15/Port:3	BLOCKED	ADSL	11/3	0/0
10.140.56.74	DEVICE04267	1	15	1	Frame:1/Slot:15/Port:1	BLOCKED	ADSL	11/1	0/0

Figure.5.23: Ports blocked for a card in OSS



IPADDRESS	ASSETNUM	FRAM	SLOT	PORT	NAME	STATUS	PORTTYPE	TAGIN	TAGOUT
10.140.56.74	DEVICE04267	1	15	2	Frame:1/Slot:15/Port:2	SPARE	ADSL	11/2	0/0
10.140.56.74	DEVICE04267	1	15	6	Frame:1/Slot:15/Port:6	SPARE	ADSL	11/6	0/0
10.140.56.74	DEVICE04267	1	15	9	Frame:1/Slot:15/Port:9	SPARE	ADSL	11/9	0/0
10.140.56.74	DEVICE04267	1	15	12	Frame:1/Slot:15/Port:12	SPARE	ADSL	11/12	0/0
10.140.56.74	DEVICE04267	1	15	18	Frame:1/Slot:15/Port:18	SPARE	ADSL	11/18	0/0
10.140.56.74	DEVICE04267	1	15	20	Frame:1/Slot:15/Port:20	SPARE	ADSL	11/20	0/0
10.140.56.74	DEVICE04267	1	15	24	Frame:1/Slot:15/Port:24	SPARE	ADSL	11/24	0/0

Figure.5.24: Ports Spare for a card in OSS

Further the status of ports being checked from the external database to know how many ports are active and how many are inactive. All the 18 ports were found active. The stop accounting and the interim accounting trends for users connecting to card number 15 is recorded.

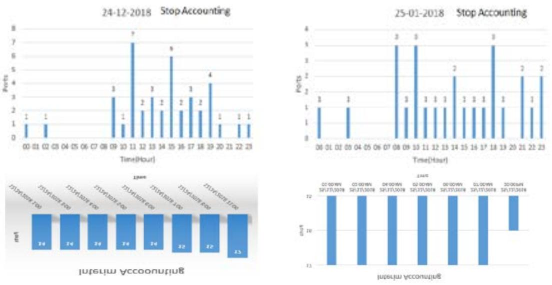


Figure.5.25: Stop and Interim accounting trend

The disconnection per hours showed variable values in Figure.5.25, this means that during 24hrs all users connected through a card may or may not disconnect during normal scenario. Then during the time period in the stop accounting where there is no disconnection the total connected user's trends can be obtained from the interim accounting. The interim accounting gives the correct Figure for the number of connected users on the resource. The data is collected for specific time based on stop accounting statistics when there was zero disconnect from users on the resource. It is observed from interim accounting that mostly users on the cards are connected (70-80%). This (70-80%) is achieved through performing analysis on interim accounting in hourly base. All trends recorded for card 15 for normal day and day when maximum disconnection observed on the card are shown in Figures (5-26,5-27,5-28,5-29,5-30,5-31). The daily trends based on stop session and interim accounting give very useful information. It can be observed from the daily trends that usually disconnection per hour is less than (70-80%) of the total card capacity we already extracted using OSS inventory and external database. The disconnection is high on 5th January (70-80%).

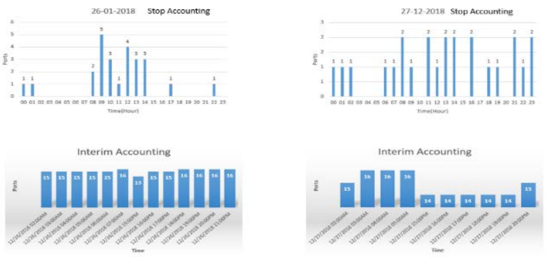


Figure.5.26 Stop and Interim accounting daily comparison-1

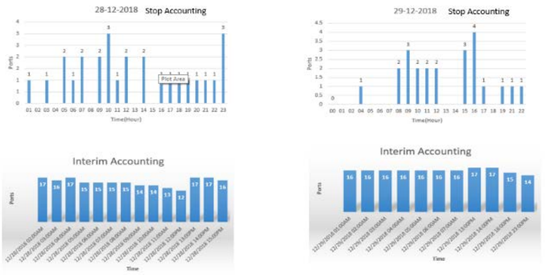


Figure.5.27 Stop and Interim accounting daily comparison-2

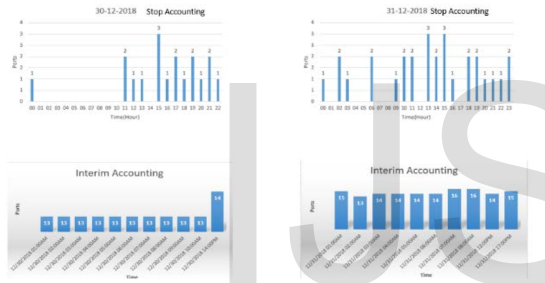


Figure.5.28 Stop and Interim accounting daily comparison-3

The figure 5.28 indicates trends for stop accounting and interim accounting for customers on one specific card. The stop accounting for users running on one card may not be triggered from the BRAS due to the reason that user are still connected and availing services. This behavior can be analyzed through viewing the interim accounting for same users running from the same card. In figure 5.28 interim accounting for same user tells that within an hour users interim accounting is recorded twice if interim time interval is configured on BRAS to 30mins. The time where there is no stop accounting the interim accounting exists, showing that mostly maximum users are connected on the network and availing services without any interruption.

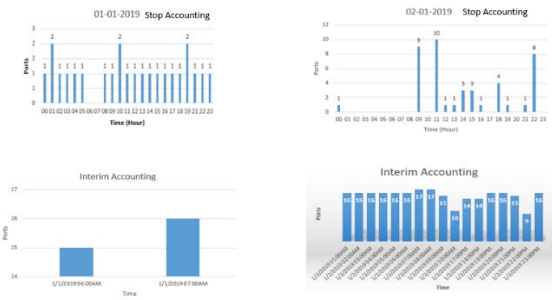


Figure.5.29 Stop and Interim accounting daily comparison-4

The figure 5.29 also indicates trends for stop accounting and interim accounting for customers on one specific card. The stop accounting for users running on one card may not be triggered from the BRAS due to the reason that user are still connected and availing services.

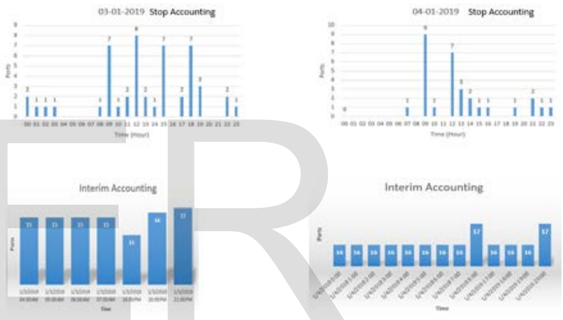


Figure.5.30 Stop and Interim accounting daily comparison -5

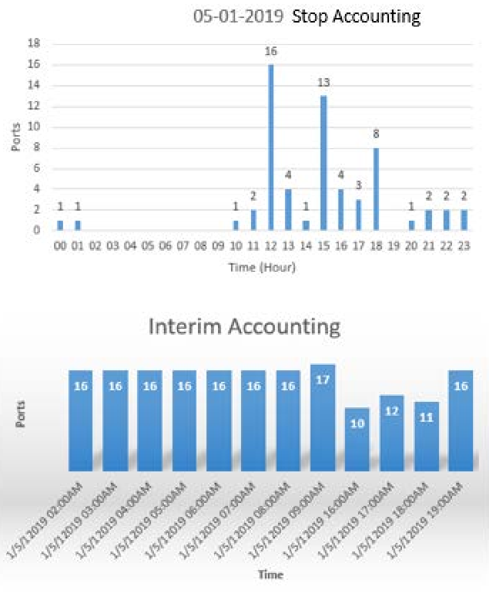


Figure.5.31 Stop and Interim trend on incident day

It is observed that instances where disconnected per hour is zero in stop accounting it does not mean that no user is connected on the card for that specific instant interim accounting trends are obtained from interim accounting table using external database. The average trend indicates that connected users per day on the basis of interim accounting per hour is around (70-80%) on a card (excluding the block port, spare ports and suspended users).

The Figure.5.31 represents the first incident occurred on the 15th card of a resource. In this incident during 1-2 minutes all the 15 connected users on the card were disconnected (80-90% of card capacity). The data is fetched from the stop accounting available in the external database shown in Figure.5.32.

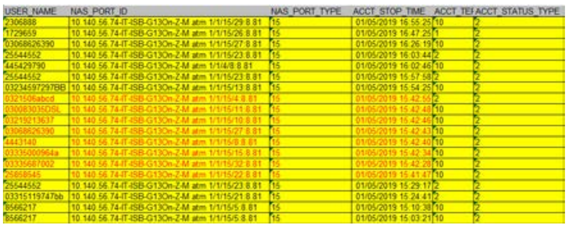
Figure.5.32 High disconnection within 2-3 minutes

All the connected users were disconnected whereas per hour interim accounting trend indicate that total connected users before the incident were 16. If previous hour interim accounting (taken as card capacity) trend is correlated to the present disconnected users 90% of disconnection is observed within 1-2 minutes. The algorithm discussed (as in chapter-4) is applied on this bulk disconnection and start accounting is checked from in the external database. It is observed that with in period less than 5-minutes all the session is reconnected and accounting start messages are received. The algorithm will point out to card reset or card reboot issue and no further checking will be carried out in this case.

Figure.5.33 High accounting start within 2-3 minutes

The above Figure.5.33 shows that in less than 5-minutes all the reinstated. It is evident from above logs that whenever a bulk disconnection is triggered due to card reset or card reboot the CPE will redial and start accounting must be triggered within 5-minutes.

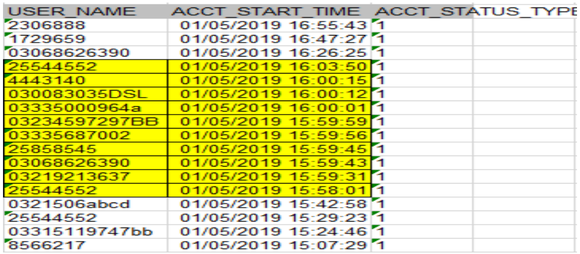
In the second incident on the card where the stop accounting referred to Figure.5.31 showed that disconnected ports within specific hour were 13 ports (60-70%) of card capacity. The records for this incidents Figure.5.34 were checked from the stop accounting in external datase. It was observed 13 ports disconnected but the number of disconnected port within 1-2 min is less than the card capacity and interim accounting trends for the users on this card. This incident doesnot refelect any outage at card level and can be ignored.



USER_NAME	NAS_PORT_ID	NAS_PORT_TYPE	ACCT_STOP_TIME	ACCT_TEI	ACCT_STATUS_TYPE
2306888	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/29:8.81	15	01/05/2019 16:55:25	10	2
1729659	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/26:8.81	15	01/05/2019 16:47:25	1	2
03068626390	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/27:8.81	15	01/05/2019 16:26:19	10	2
25544552	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/23:8.81	15	01/05/2019 16:03:44	2	2
445429790	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/4/8:8.81	15	01/05/2019 16:02:46	10	2
25544552	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/23:8.81	15	01/05/2019 15:57:58	2	2
03234597297BB	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/13:8.81	15	01/05/2019 15:54:25	10	2
0321506abcd	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/4:8.81	15	01/05/2019 15:42:56	2	2
030083035DSL	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/11:8.81	15	01/05/2019 15:42:48	10	2
03219213637	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/10:8.81	15	01/05/2019 15:42:46	10	2
03068626390	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/27:8.81	15	01/05/2019 15:42:43	10	2
4443140	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/8:8.81	15	01/05/2019 15:42:40	10	2
03335000964a	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/15:8.81	15	01/05/2019 15:42:34	10	2
03335687002	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/32:8.81	15	01/05/2019 15:42:28	10	2
25858545	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/22:8.81	15	01/05/2019 15:41:47	10	2
25544552	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/23:8.81	15	01/05/2019 15:29:17	2	2
03315119747bb	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/21:8.81	15	01/05/2019 15:24:41	2	2
8566217	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/5:8.81	15	01/05/2019 15:10:38	10	2
8566217	10.140.56.74-IT-ISB-G13On-Z-M atm 1/1/15/5:8.81	15	01/05/2019 15:03:21	10	2

Figure.5.34 High disconnection within an hour but less port resets

The start accounting records for same incident as presented by Figure.5.35 showed that the users were not connected immediately after the stop incident was triggered (< 5mins) and this incident does not represent the bulk disconnection (This was no start accounting from disconnected users after 15:42:58 till 15:58:01). Such kind of issue's may points to some local issue at the customer side or due to power outage in some area some of the users got disconnected but other remain connected on the card.



USER_NAME	ACCT_START_TIME	ACCT_STATUS_TYPE	
2306888	01/05/2019 16:55:43	1	
1729659	01/05/2019 16:47:27	1	
03068626390	01/05/2019 16:26:25	1	
25544552	01/05/2019 16:03:50	1	
4443140	01/05/2019 16:00:15	1	
030083035DSL	01/05/2019 16:00:12	1	
03335000964a	01/05/2019 16:00:01	1	
03234597297BB	01/05/2019 15:59:59	1	
03335687002	01/05/2019 15:59:56	1	
25858545	01/05/2019 15:59:45	1	
03068626390	01/05/2019 15:59:43	1	
03219213637	01/05/2019 15:59:31	1	
25544552	01/05/2019 15:58:01	1	
0321506abcd	01/05/2019 15:42:58	1	
25544552	01/05/2019 15:29:23	1	
03315119747bb	01/05/2019 15:24:46	1	
8566217	01/05/2019 15:07:29	1	

Figure.5.35 Delayed start accounting for disconnected users

The Figure.5.36 best explains that the issue was not at card level as during the second incident all the users connected on the cards were not disconnected. The sample case shows that the user was connected from 05-01-2019 15:24:46 and disconnected after two days (07-01-2019 07:45:13)

Figure.5.36 All users not disconnected on the card

Both the incidents indicate that whenever a card is rebooted or reset it can be tracked using the accounting information available in the database in real-time. All the customers connected on the card will be disconnected (70-80%) at once and after few minutes there will be start accounting records for disconnected users in the external database indicating that card was reset or rebooted. In the other case if not all the users running from the card are disconnected then it can be ignored as it does not indicate any problem with respect to the card.

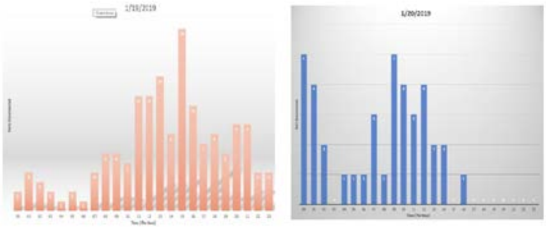


Figure.5.37 Daily trends for port disconnection on a card (Per hour)

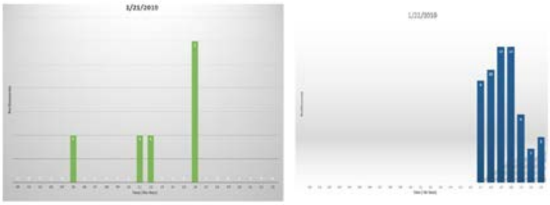
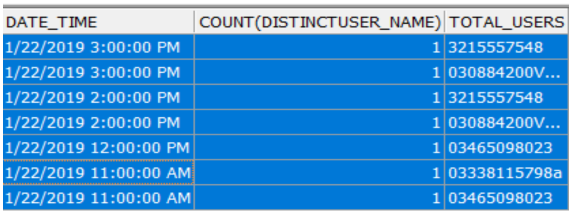


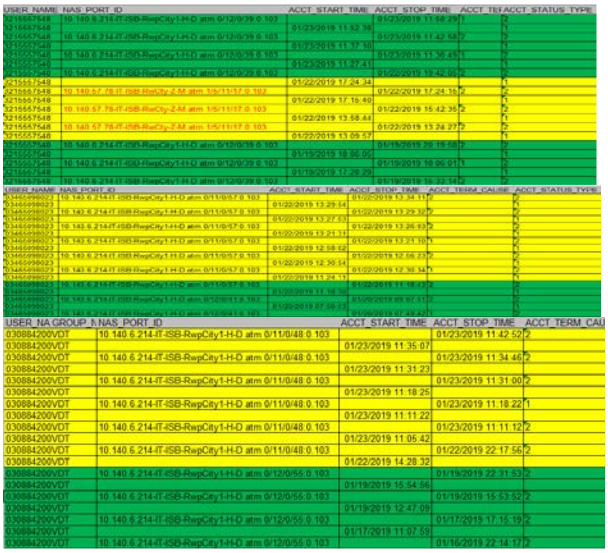
Figure.5.38 Recorded Trend during and after incident

Similarly, there was another issue appeared on a different card that can be tracked properly using the algorithm applied in this research. To fix certain complaints for users running from a specific card it is administrated rebooted or it is physically reinserted in the slot due to this reason sometime cards went into abnormal state or subscribers trying to connect are not able to authenticate but at card level and resource level everything seems fine. Such scenarios can be pointed out in timely manner using the accounting information in real time.



DATE_TIME	COUNT(DISTINCTUSER_NAME)	TOTAL_USERS
1/22/2019 3:00:00 PM	1	3215557548
1/22/2019 3:00:00 PM	1	030884200V...
1/22/2019 2:00:00 PM	1	3215557548
1/22/2019 2:00:00 PM	1	030884200V...
1/22/2019 12:00:00 PM	1	03465098023
1/22/2019 11:00:00 AM	1	03338115798a
1/22/2019 11:00:00 AM	1	03465098023

Figure.5.39 Interim records during incident time for card shifted cases



USER_NAME	NAS_PORT_ID	ACCT_START_TIME	ACCT_STOP_TIME	ACCT_TEF	ACCT_STATUS_TYPE
3215557548	10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/39:0.103		01/23/2019 11:58:29	1	2
3215557548		01/23/2019 11:52:38			1
3215557548	10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/39:0.103		01/23/2019 11:42:58	2	2
3215557548		01/23/2019 11:37:18			1
3215557548	10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/39:0.103		01/23/2019 11:36:45	1	2
3215557548		01/23/2019 11:27:41			1
3215557548	10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/39:0.103		01/22/2019 19:42:05	2	2
3215557548		01/22/2019 17:24:34			1
3215557548	10.140.57.78-IT-ISB-RwCity-Z-M atm 1/5/11/17:0.102		01/22/2019 17:24:15	2	2
3215557548		01/22/2019 17:16:40			1
3215557548	10.140.57.78-IT-ISB-RwCity-Z-M atm 1/5/11/17:0.103		01/22/2019 15:42:35	2	2
3215557548		01/22/2019 13:58:44			1
3215557548	10.140.57.78-IT-ISB-RwCity-Z-M atm 1/5/11/17:0.103		01/22/2019 13:24:27	2	2
3215557548		01/22/2019 13:09:57			1
3215557548	10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/39:0.103		01/19/2019 20:18:58	2	2
3215557548		01/19/2019 18:06:05			1
3215557548	10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/39:0.103		01/19/2019 18:06:01	1	2
3215557548		01/19/2019 17:28:29			1
3215557548	10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/39:0.103		01/19/2019 16:33:14	2	2

USER_NAME	NAS_PORT_ID	ACCT_START_TIME	ACCT_STOP_TIME	ACCT_TERM_CAUSE	ACCT_STATUS_TYPE
03465098023	10.143.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/57:0.103		01/22/2019 13:34:11	2	2
03465098023		01/22/2019 13:29:54			1
03465098023	10.143.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/57:0.103		01/22/2019 13:29:32	2	2
03465098023		01/22/2019 13:27:53			1
03465098023	10.143.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/57:0.103		01/22/2019 13:26:03	2	2
03465098023		01/22/2019 13:21:11			1
03465098023	10.143.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/57:0.103		01/22/2019 13:21:10	1	2
03465098023		01/22/2019 12:58:02			1
03465098023	10.143.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/57:0.103		01/22/2019 12:56:23	2	2
03465098023		01/22/2019 12:30:54			1
03465098023	10.143.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/57:0.103		01/22/2019 12:30:34	1	2
03465098023		01/22/2019 11:24:11			1
03465098023	10.143.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/57:0.103		01/22/2019 11:18:43	2	2
03465098023		01/22/2019 11:16:38			1
03465098023	10.143.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/41:0.103		01/20/2019 09:07:51	2	2
03465098023		01/20/2019 07:50:03			1
03465098023	10.143.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/41:0.103		01/20/2019 07:43:42	1	2

USER_NA	GROUP_N	NAS_PORT_ID	ACCT_START_TIME	ACCT_STOP_TIME	ACCT_TERM_CAU
030884200VDT		10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/48:0.103		01/23/2019 11:42:52	2
030884200VDT			01/23/2019 11:35:07		
030884200VDT		10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/48:0.103		01/23/2019 11:34:46	2
030884200VDT			01/23/2019 11:31:23		
030884200VDT		10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/48:0.103		01/23/2019 11:31:00	2
030884200VDT			01/23/2019 11:18:25		
030884200VDT		10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/48:0.103		01/23/2019 11:18:22	1
030884200VDT			01/23/2019 11:11:22		
030884200VDT		10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/48:0.103		01/23/2019 11:11:12	2
030884200VDT			01/23/2019 11:05:42		
030884200VDT		10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/11/0/48:0.103		01/22/2019 22:17:56	2
030884200VDT			01/22/2019 14:28:32		
030884200VDT		10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/55:0.103		01/19/2019 22:31:53	2
030884200VDT			01/19/2019 15:54:56		
030884200VDT		10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/55:0.103		01/19/2019 15:53:52	2
030884200VDT			01/19/2019 12:47:09		
030884200VDT		10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/55:0.103		01/17/2019 17:15:19	2
030884200VDT			01/17/2019 11:07:59		
030884200VDT		10.140.6.214-IT-ISB-RwpCity1-H-D atm 0/12/0/55:0.103		01/16/2019 22:14:17	2

Figure.5.40 Users services shifted to different card during incident

The 12th card was not working properly due to this all the customers on this card were suffering. Some of the users were shifted to other card to run the services till the card is restored. The applied algorithm can also help in shifting the services of affected customer to another card if the issue is not restored in committed time. The figure.5.39 points to users for which services were shifted to some another adjacent card due to which during the incident duration (when 12th card was faulty) the interim accounting for few users was coming in the external database. When analysis was carried out on such users during the incident time it was observed to restore the services for some customers they were shifted to another card (11th card) but other customers' services were not restored and from them this issue lasted for more almost two days. In author opinion in case of prolonged issues spare ports can be used to shift the services it can be achieved if proper end-to-end monitoring system is deployed.

Conclusion and Future Work

The suggested solution in this work using the provisioning system, External database and BI analytics shows high amount of accuracy in estimation of active ports on which customer is provisioned and configured and using services. It also enables operator to filter ports on which customers are suspended due to non-payment using external database. Applying the suggested above algorithm on activated ports significantly enhance monitoring huge PPP failures. The accounting information triggered from RADIUS servers to External DB are processed in real time by BI system. The reports generated at BI systems are dispatched to the concern vendors, system owners and management as part of escalation process. This implementation will help a telecommunication operator to respond to any unforeseen situation more efficiently before the customer register the complaint.

The solution discussed will not absolute other monitoring solution but is a source of additional monitoring for scenarios where alters are not triggered but bulk disconnection requests are received by radius server and information is recorded in database. This additional reporting at BI level will assist operators to respond to such incidents more quickly.

References

[1] Zych P, "Network Failure Detection Based on Correlation Data Analysis" in International Journal of Electronics and Communication (AUE),2017

[2] C Rigney, AC Rubens, WA Simpson, S Willens, "RFC2865 – Remote Authentication Dial In User Service (RADIUS)", IETF; 1997

[3] F Baker, "RFC1661 – The Point-to-Point Protocol (PPP)", IETF; 1994

[4] Chu W, Guan X, Cai Z, Gao L. "Real-time volume control for interactive network traffic replay". Comput Netw 2013;57(7):1611–29. http://dx.doi.org/10.1016/j.comnet.2013.02.012

[5] J.Kerpez K, Galli S, Ginis G, Goldburg M, J.Silverman P, Mohseni M, "Method And Apparatus For Diagnosing And Configuring A Broadband Connection via An Artificial Communication Path", US Patent 9860111 B2;2018

[6] Kuipers M, Data processing in a digital subscriber line environment, US Patent 9973634 B2; 2018.

[7] R.Groves Vernon,W.Scott Justin, Greene Dylan, Large-scale passive network monitoring using multiple tires of ordinary network switches, US Patent 10091073 B2, 2018.

[8] F.Abdulnour M, L.Hume K, A.Ronald P, T.Whittal P, Data communications performance monitoring, US 10153950 B2, 2018.

[9] Gedge R, Barnett S, Optimised broadband line testing, US Patent 9998590 B2,2018.

[10] Paul S, Kumar S. Comparative analysis of various PPP authentication Protocols. International journal of innovative research in computer and Communication Engineering 2017;1399-1404 https://doi.org/10.15680/IJIRCCE.2017

[11] Kim M, Kim S, Kong AJ. High performance AAA architecture for massive IPv4 networks. Future Gen Comput Syst 2006;23(2):275–9. http://dx.doi.org/10.1016/j.future.2006.05.003.

[12] Lee S, Levanti K, Kim HS. Network monitoring: present and future. Comput Netw 2013; 65:84–98. http://dx.doi.org/10.1016/j.comnet.2014.03.007

[13] Patil VU, Kapur AR. Real time alert data acquisition system using dynamic IP embedded webserver by USB modem. Proc Comput Sci 2015;49:187–93. http://dx.doi.org/10.1016/j.procs.2015.04.243.

[14] Fardid R, Systems and method for Automated Monitoring of availability in XDSL access networks, US Patent 7099305 B1, 2006

[15] M.Croot C, P.Linney T, W.Cook J, Monitoring data communication in an access network, US Patent 8537701 B2, 2013

[16] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[17] Vierhauser M, Rabiser R, Grunbacher P, Seyerlehner K, Wallner S, Zeisel H.ReMinds: A flexiable runtime monitoring framework for systems of systems. The Journal of Systems and Software 2015; 000():1-14

[18] P.DeHaan M, K.Likins A, K.Vidal S, Detecting Network Conditions Based on Correlation between Trends Lines, US Patent 9967169 B2, 2018.

[19] Mishra R, Buchner M, H.Graham J, Glendinning, Geyer M, Pope K., R.Ettle D, Architecture for operational support system, US Patent 9660868 B2, 2017.

[20] Isik O, C.Jones M, Sidorova A: Business intelligence success: The roles of BI capabilities and decision environments. Information and Management 2013;50( ):13-23

[21] Acker O, Grone F, Blockus A, Bange C. In-memory analytics -Strategies for real-time CRM. Database Marketing & Customer Strategy Management 2011; vol 18(2):129-136

[22] A.Aderemi A, P.Segun I, A.Oluwaseun J, A.David G, A.Matthew B, Adetola Victor, Adetiba Emmanuel, " Trends and patterns of broadband Internet access speed in a Nigerian university campus:A robust data exploration", Data in Brief;2019.

[23] Q.Wander, C.Miriam A.M, D.Mario, " An approach for SDN traffic monitoring based on big data techniques", Journal of Network and Computer Applications;2019

[24] M. Ferrazani D.M, D.Bandeira O. C, " AuthFlow: authentication and access control mechanism for software defined networking" in Institut Mines-Tel ´ ecom and Springer-Verlag France, 2016

[25] Lv Bin, Yu Xuemin, Xu Guokun, Yin Qilei, Shi Zhixin, " Network Traffic Monitoring System Based on Big Data Technology", Association for Computing Machinery; ICBDC '18, April 28–30, 2018.

[26] Deljac Z, Randic M, Krcelic G, " A Multivariate Approach to Predicting Quantity of Failures in Broadband Networks Based on a Recurrent Neural Network", J Netw Syst Manage; 2015.

[27] Maccari L, Passerini A. "A Big Data and machine learning approach for network monitoring and security". Security and Privacy 2018;e53. https://doi.org/10.1002/spy2.53

[28] Pham H.John, Clark J.Clayton, "Method and System For Performance Monitoring of Network Terminal Devices", US Patent 8966555 B2; 2015.

[29] Voit E, Pruss R.Manfred, Hertoghs Y, Evans J.Willian, "Quality of Service Based on Logical Port Identified For Broadband Aggregation Networks", US Patent 9088619 B2;2015.

[30] Compann J, Helms K.Scott, "Broadband Diagnostics System", US Patent 9112718 B2; 2015.

[31] P.Solthouber L,"Network Bandwidth Regulation Using Traffic Scheduling", US 8937866 B2; 2015.

[32] Dillon D, "System and Method For Providing Improved Quality of Service over Broadband Networks", US 9716659 B2; 2017.

[33] J.Kerpez K, Galli S, Ginis G, Goldburg M, J.Silverman, Mohseni M, " Method and Appratus for Diagnosing and Configuring a Broadband and Connecting Via an Alternatate Communication Path", US 9860111 B2; 2018.

[34] Bednarz P, Cil T, Tehrani A.Maleki, Dagum L, Goldburg M, "Method and Appratus for Cloud Services For Enhancing Broadband Experience", US 9967156 B2; 2018.

[35] Lee W, Amde M, Ginis G, "System and Method For Validationg Broadband Service Recommendation", US 10020999 B2; 2018.

[36] Linney T, Horsley I, "Digital Subscriber Line Profile Selection Method and Apparatus", US 10142489 B2; 2018.

[37] Abdulnour M.Fakkar, Hume K.Louise, Ronald P.Alan, Whittall P.Trevor, " Data Communications Performance Monitoring", US 10153950 B2; 2018.