Network Alarm Overload Analysis

(Machine Learning Approach)

Chandrashekar V & Devesh Srivastava
December, 2016

Contents


POLICE

Need for preventive solution in network domain

- Lost sales revenue
- Lost employee productivity
- Cost to restore IT systems
- Financial impact of customer dissatisfaction
- Contract penalties
- Potential litigation/loss of stock value
- Missed deadlines that result in employee overtime

Source - https://support.rackspace.com

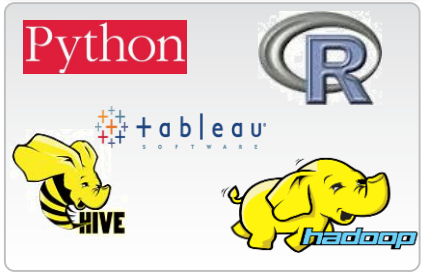
Overview

"Too many Alarms is just the symptom, not the problem "

Key Stats

- Thousands of Alarms flowing
- ~1000 Devices generating hundreds of events every second

Tools & Techniques Used



Business Problem

- Information overload : Lot of Alarms may be missed due to the sheer volumes or inefficient Alarm rules
- Impractical to manually analyze the alarms cause and effect

Solution

- Intelligent machine learning based system to identify events that are "redundant" from those that are critical to the Network operations and security
- Using Association Rule Mining algorithms, we have grouped the events using a Sliding Window methodology to get associations between related episodes generated by Syslog messages
- We can find alarm patterns that are "redundant" and also the ones that are not obvious but critical ones that affect the network

Results

- Algorithms built: e.g: By analyzing patterns and relations, established rules that will be tested: If alarm A occurs, then alarm E and G are likely to occur at "x" and "y" time instance

Key Challenges

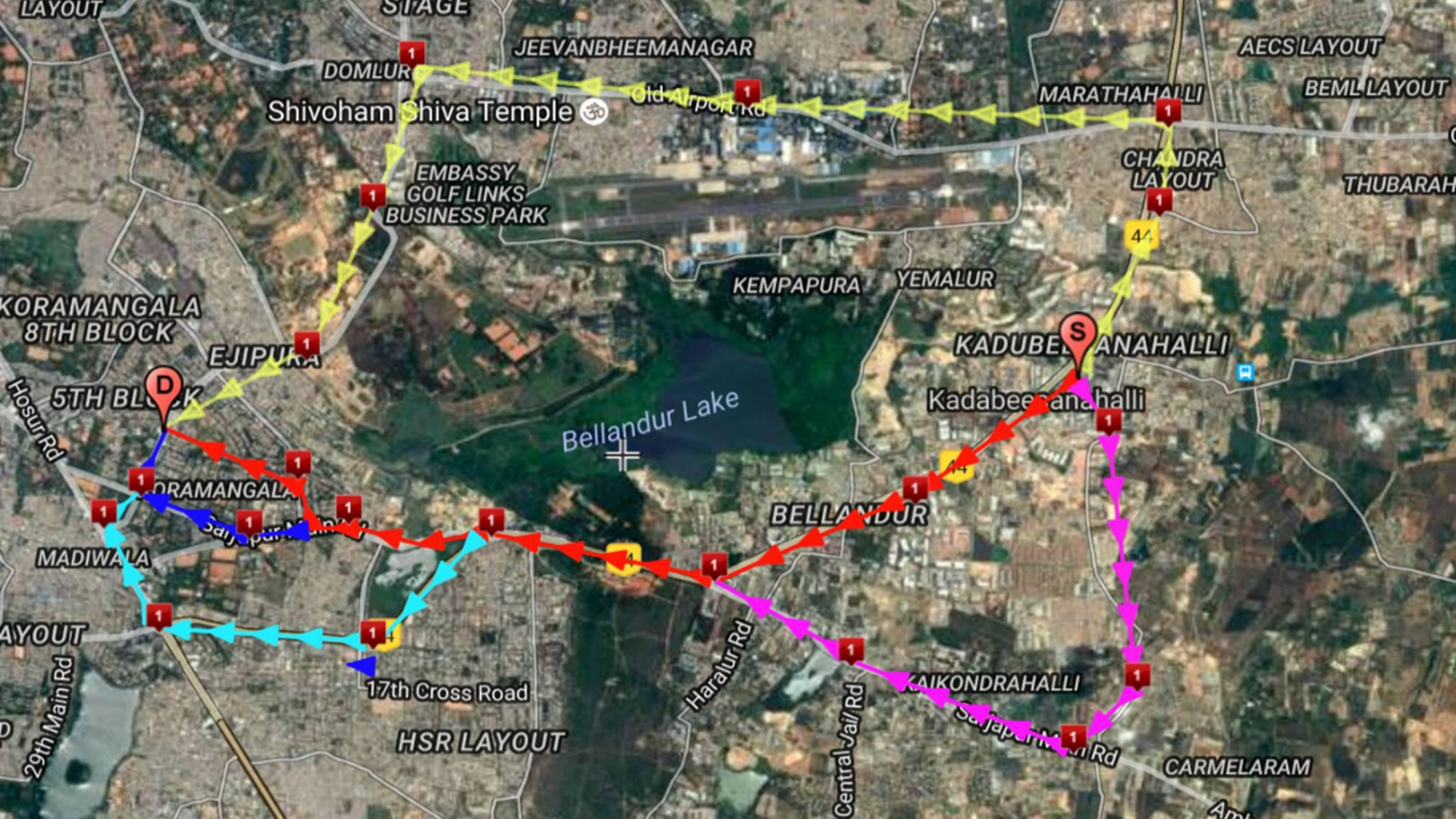
•Mining large volumes of network events to generate significant rules

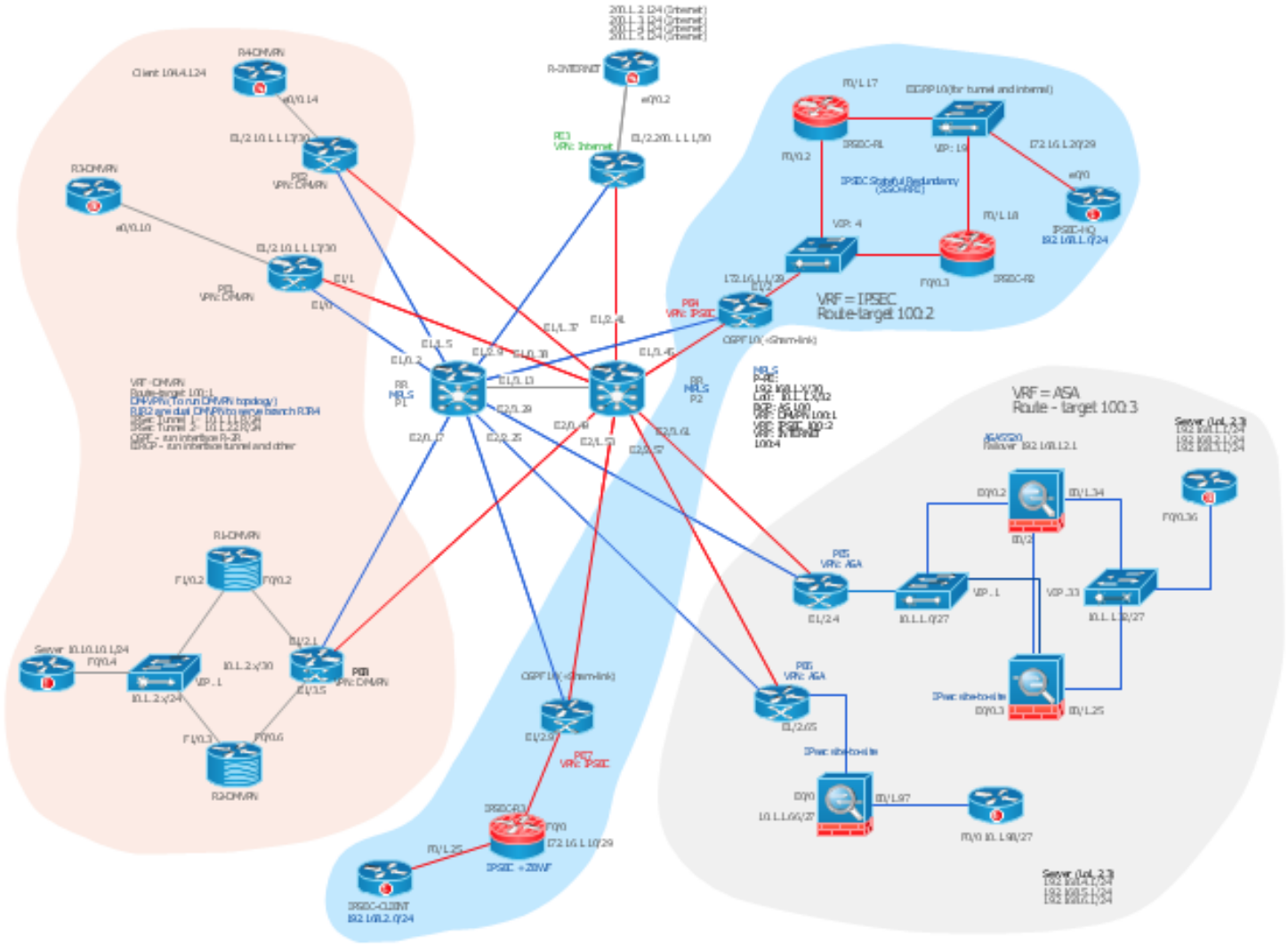
•Identifying related events within duration of a few seconds minutes over a period of 1 year

•Discovering rare events that are critical to network health

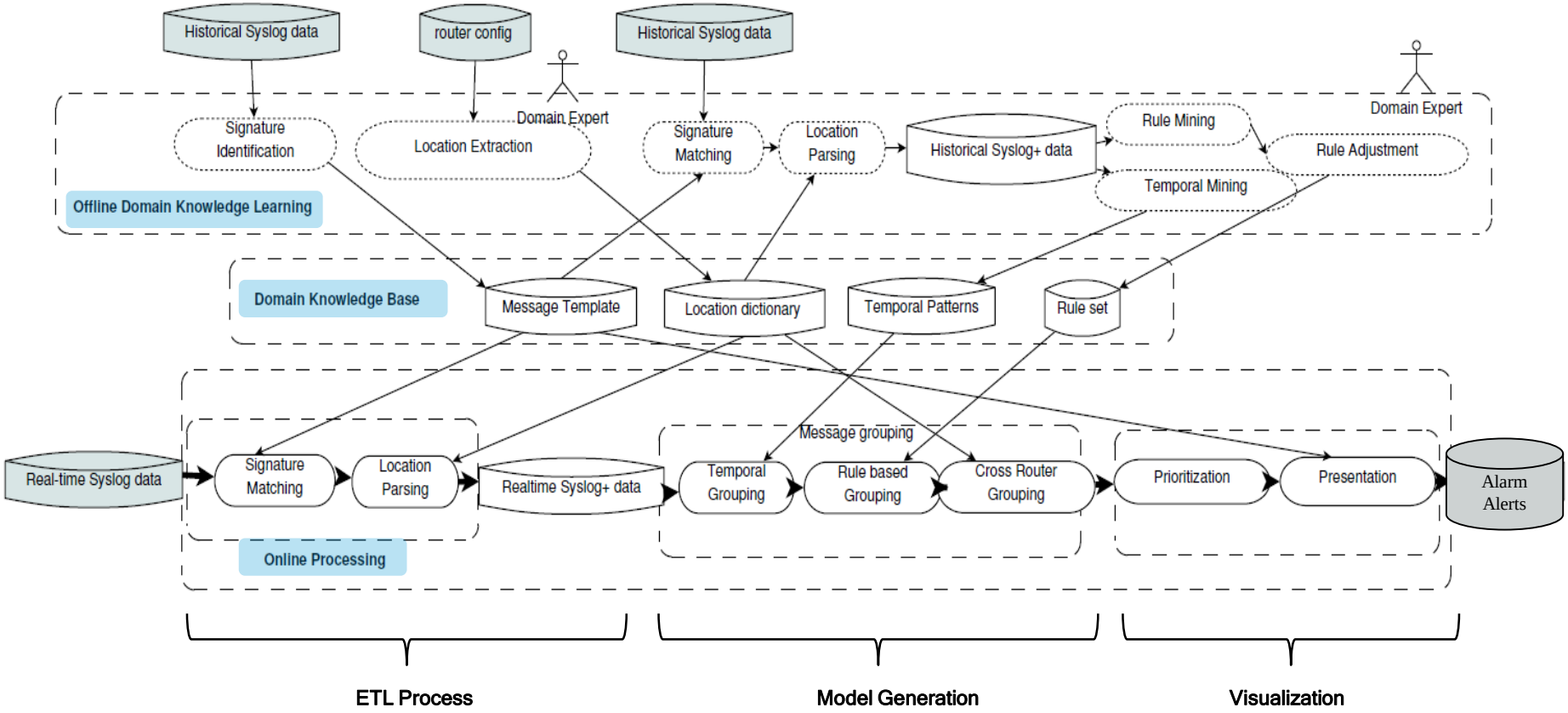
•Grouping the devices on a relevant

•Pattern mining the generated rules on a time scale


JEEVANBHEEMANAGAR
DOMLUR
Shivoham Shiva Temple
Old Airport Rd
AECS LAYOUT
BEML LAYOUT
MARATHAHALLI
CHANDRA LAYOUT
THUBARAHALLI
EMBASSY GOLF LINKS BUSINESS PARK
KEMPAPURA
YEMALUR
KORAMANGALA 8TH BLOCK
EJIPURA
KADUBEESANAHALLI
Kadabeesanahalli
5TH BLOCK
Hosur Rd
Bellandur Lake
BELLANDUR
MADIWALA
17th Cross Road
HSR LAYOUT
29th Main Rd
Haralur Rd
Central Jail Rd
KAIKONDRAHALLI
CARMELARAM


VRF = IPSEC
Route-target 100:2
VRF = ASA
Route - target 100:3
VRF : CMVRN
Route-target 100:1
CMVRN (To run CMVRN topology)
BGP2 are dual CMVRN to serve branch R3&4
Client Tunnel 1 : 10.1.1.0/24
Client Tunnel 2 : 10.1.2.0/24
OSPF - run interface R-2R
EIGRP - run interface tunnel and other
R4-CMVRN
R3-CMVRN
R1-CMVRN
R2-CMVRN
R-INTERNET
R3
VRF: Internet
PE1
VRF: CMVRN
PE2
VRF: CMVRN
PE3
VRF: CMVRN
PE4
VRF: IPSEC
PE5
VRF: ASA
PE6
VRF: ASA
PE7
VRF: IPSEC
RR
MPLS
P1
RR
MPLS
P2
OSPF 10 (<2km+link)
IPSEC-HQ
IPSEC-R1
IPSEC-R2
IPSEC-R3
IPSEC-CLIENT
IPSEC + 2DMF
ASA5520
Failover
Server (Lo1, 2, 3)
Server 10.10.10.1/24
IPsec site-to-site
IPsec site-to-site
VIP: 1
VIP: 4
VIP: 19
VIP: 33
EIGRP 10 (for tunnel and internal)
OSPF 10 (<2km+link)

Solution Design



Rules Generation

What is the presumption behind the Association Rule Generation?

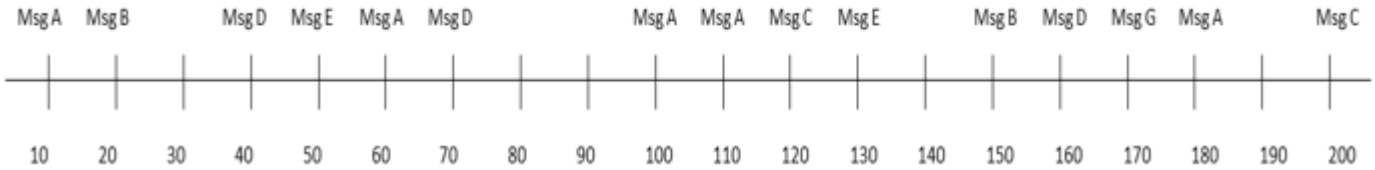
- Association rules describe how things occur together in the data

  E.g., "IF an alarm has certain properties, THEN it will have other given properties"

- Episode rules describe temporal relationships between things

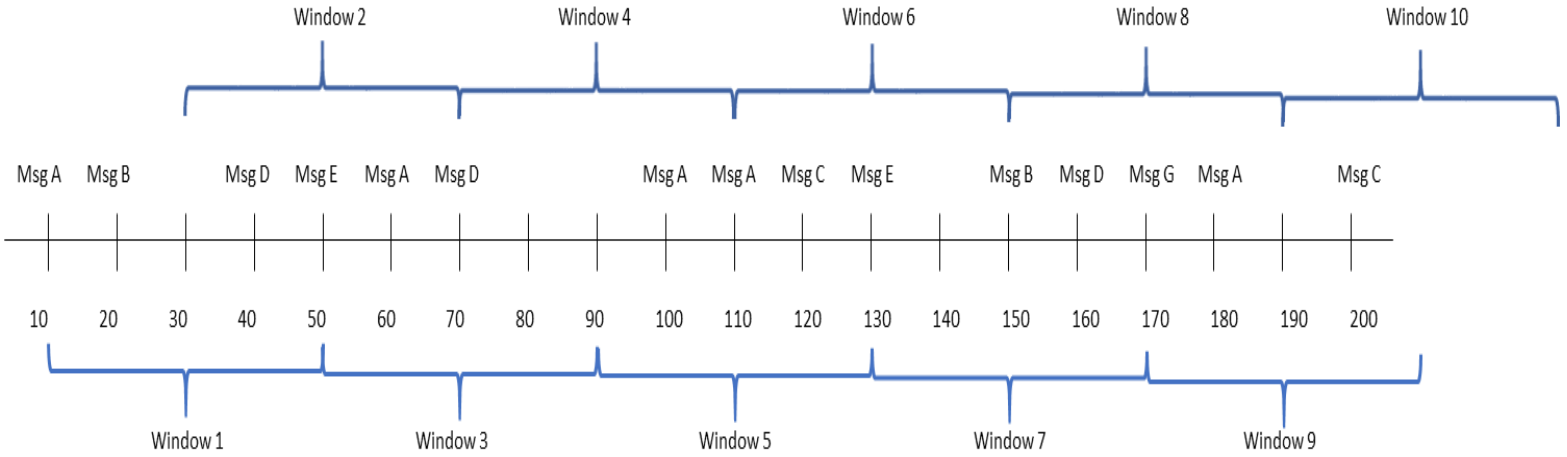
  E.g., "IF a certain combination of alarms occurs within a time period, THEN another combination of alarms will occur within a time period"

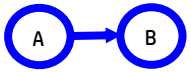
- In this scenario, we face a challenge of identifying “transactions” relevant for association rules

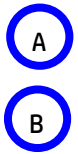


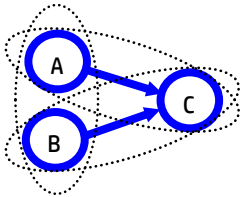
  - *MsgA, MsgB….* are event (or here msg) types
  - *10…200* are occurrence times
  - There is a possibility of using the time-windows suitable length to group transactions
  - What is a suitable length?

A mechanism for transaction identification using Sliding Windows



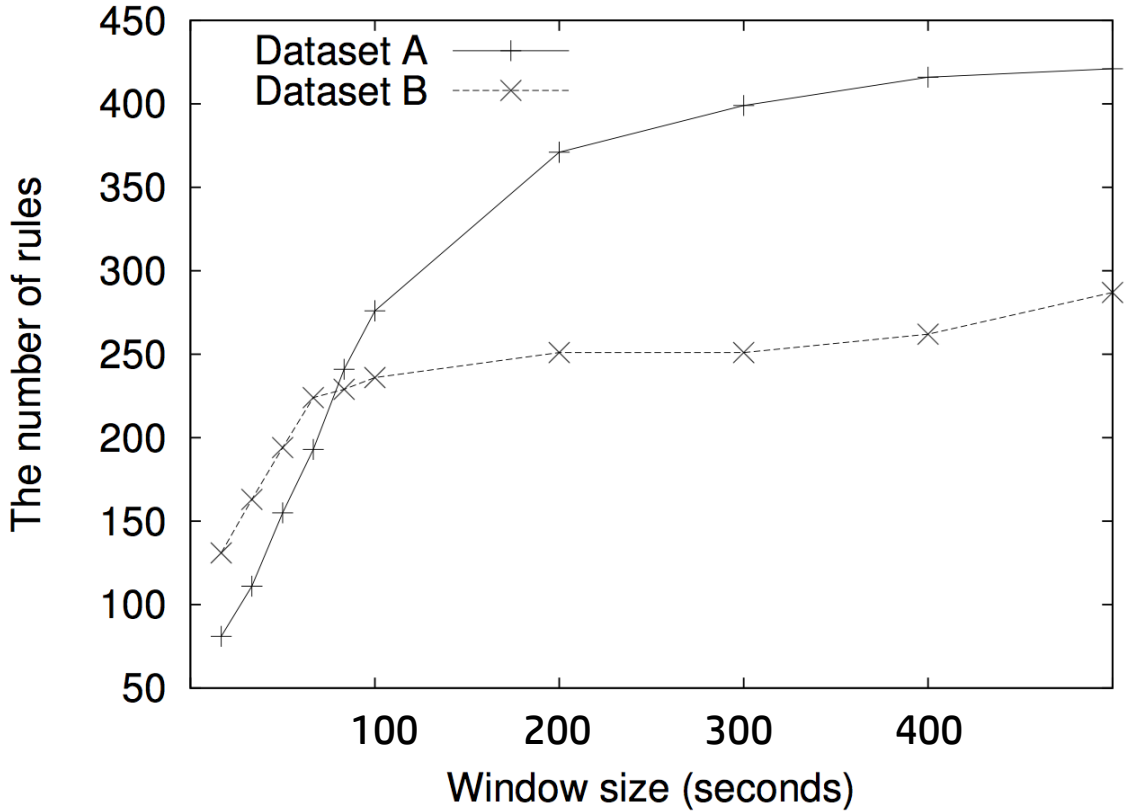






- Using these windows are transactions, we can group them into individual transactions amenable for Association Rule Mining
- Moving the sliding windows by half of the window length allows us to cover overlapping transactions efficiently

Appropriate window size



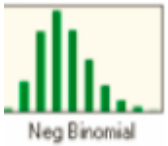
Model Selection (apriori vs arulesnbminer)

Problems with apriori

- Support is prone to the rare item problem where associations including items with low support are discarded although they might contain valuable information.
- Support favors smaller item sets while longer item sets could still be interesting, even if they are less frequent. In order to find longer item set, one would have to lower the support threshold which would lead to an explosion of the number of short item sets found.

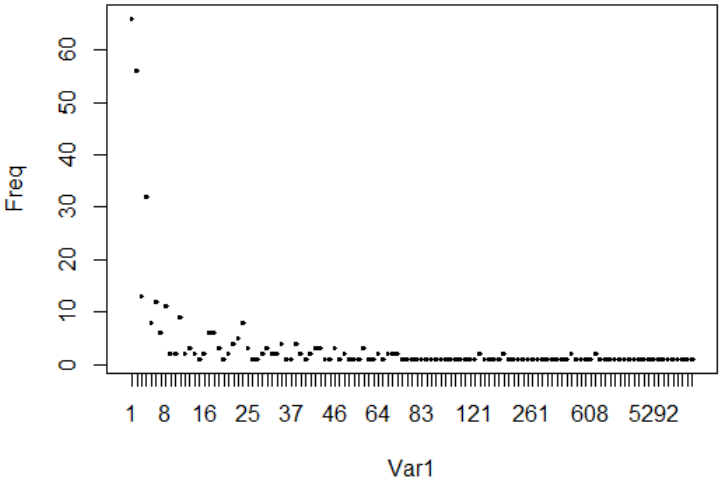
Nbminer as solution

- It reduces the problem with rare items since the used stochastic model allows for highly skewed frequency distributions.
- It is able to produce longer associations without generating an enormous number of shorter, spurious associations since the support required by the model is set locally and decreases with the number of items forming an association.
- Its precision threshold parameter can be interpreted as a predicted error rate. This makes communicating and setting the parameter easier for domain experts. Also, the parameter seems to be less dependent on the structure of the database than support.

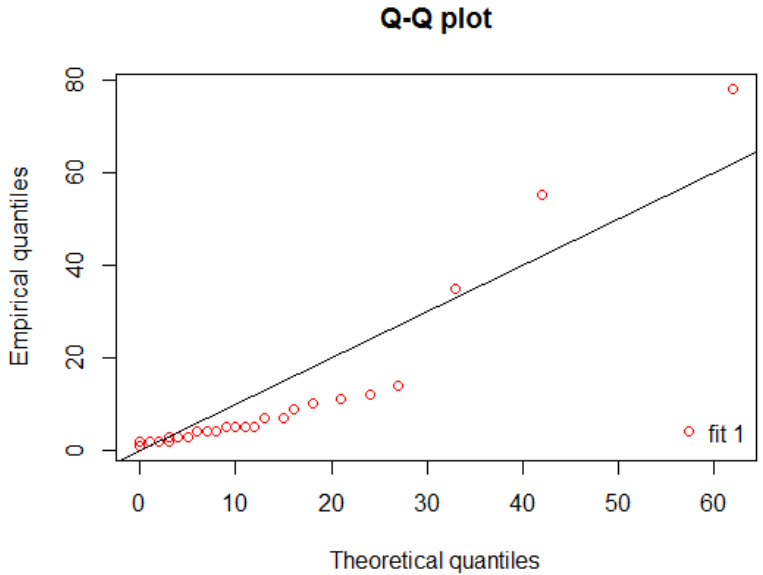


Fitting the Negative Binomial distribution to our data

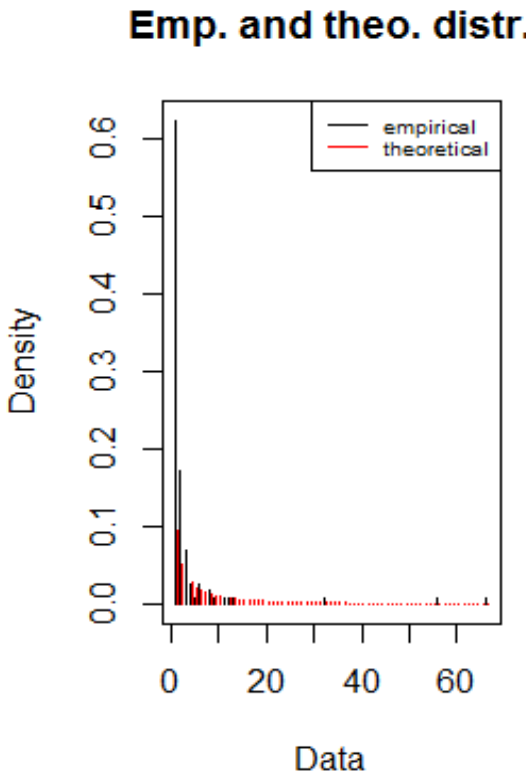
Distribution of Message Type counts looks like a fit for NB model

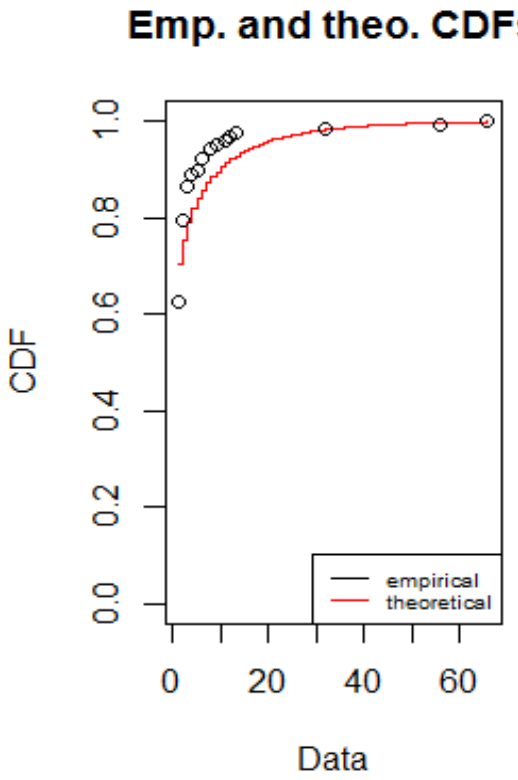



```
Fitting of the distribution ' nbinom ' by matching moments

Parameters : estimate size 0.1620777 mu 3.3076923

Loglikelihood: -336.9997 AIC: 677.9993 BIC: 683.5237
```

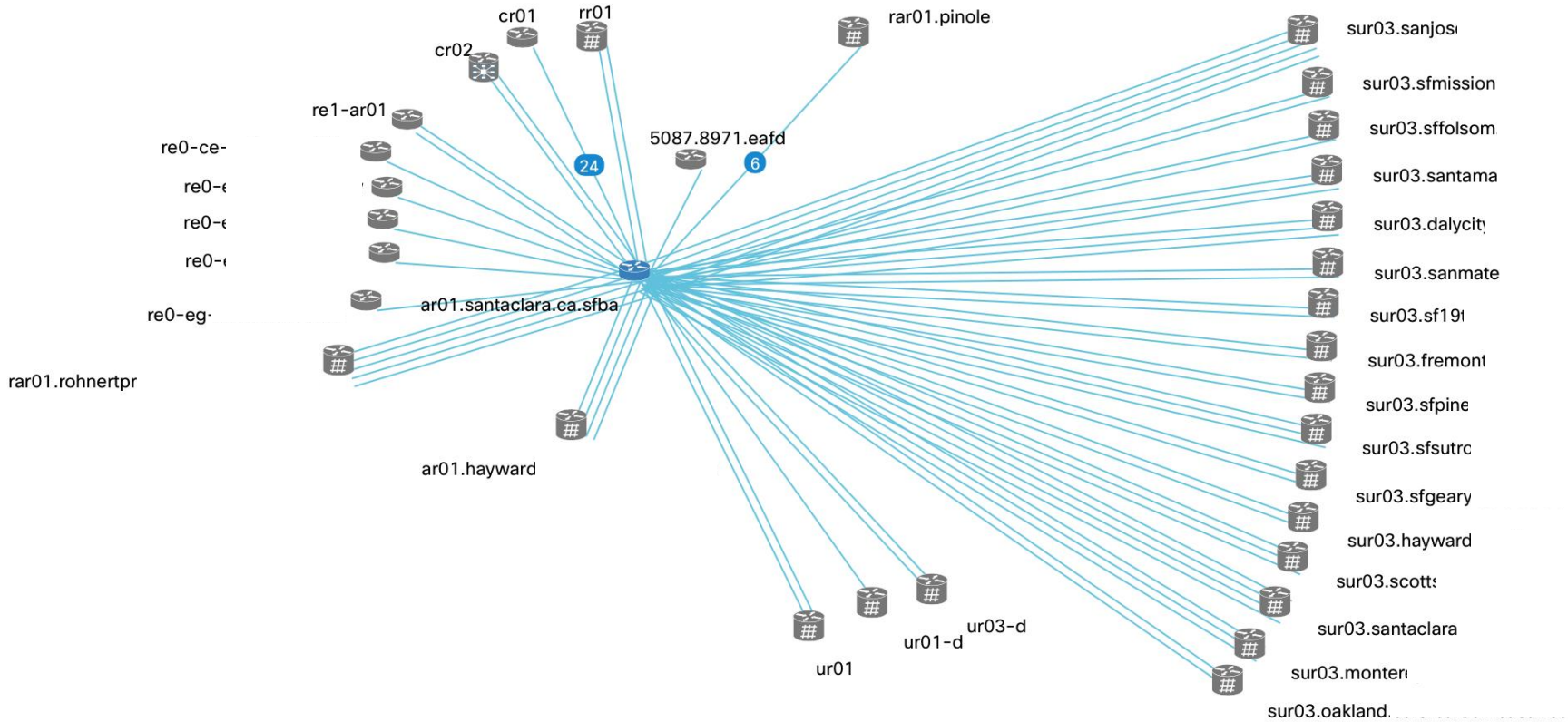


Fitting the Negative Binomial distribution to our data

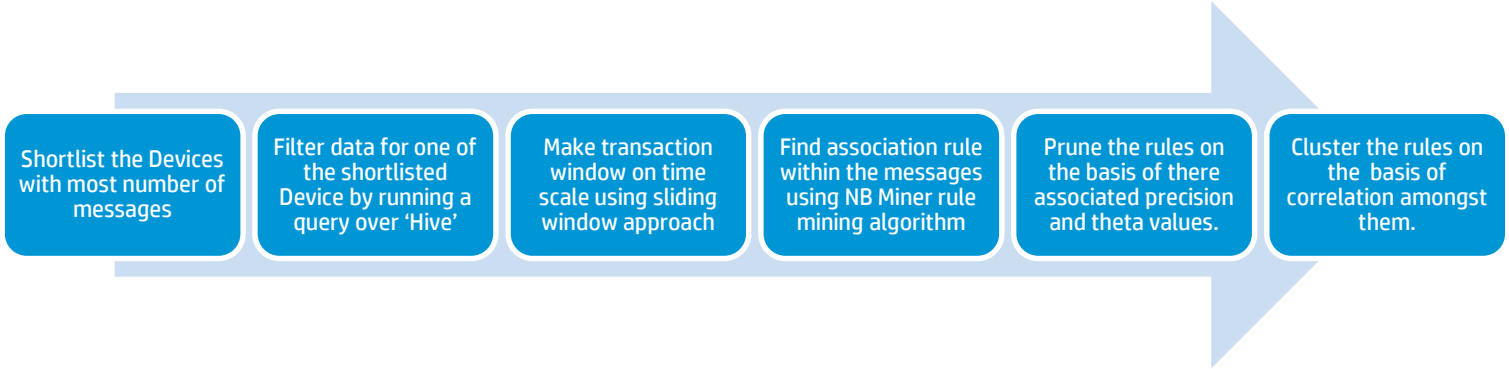




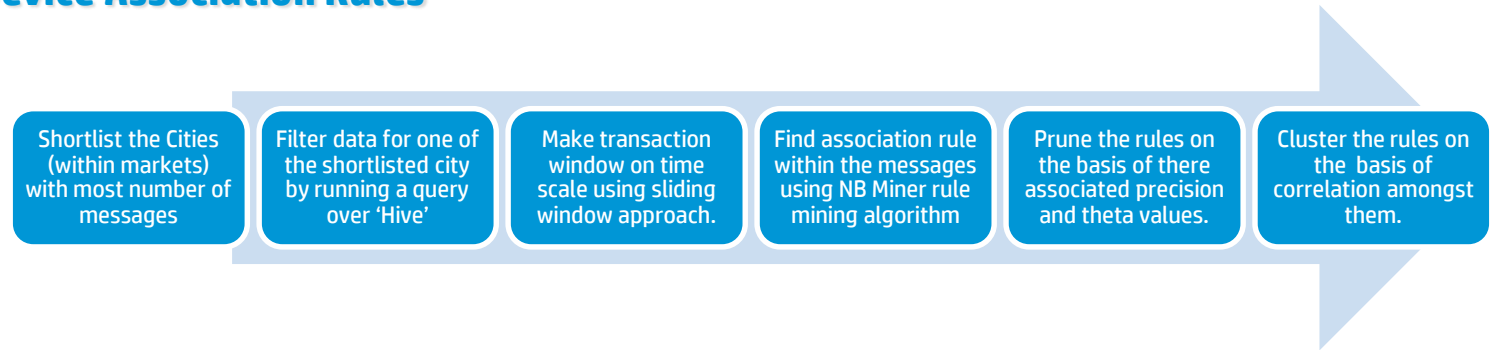
Location Dictionary (Network Neighbor Topology)



Intra Device Association Rules



Inter Device Association Rules



Rule Creation

Optimized Syslog				
	mtprospect.il.Chicago	springfield.il.chicago	wchicago.il.chicago	mtprospect.il.ndcnorth
Messages	178864	174709	183501	288810
Episodes	55291	55298	55302	18429
Overall Rules	12873	2325	7154	2590
Filtered Rules	711	419	2253	1688

Sample Rule :

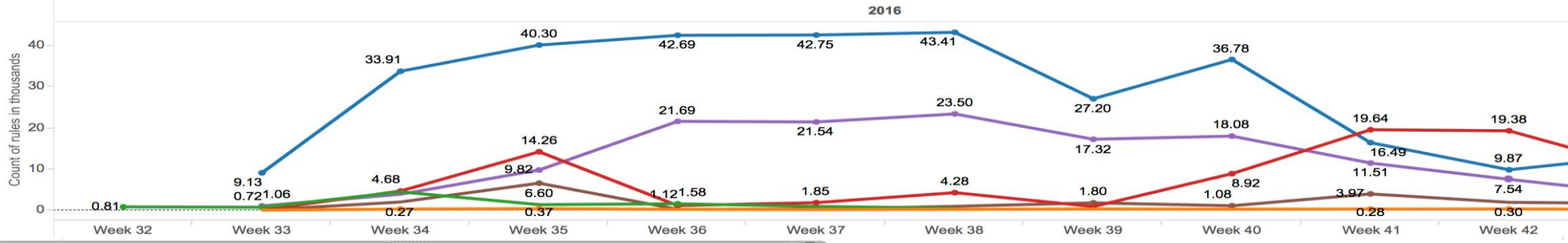
L2-L2VPN_PW-3-UPDOWN-sur03.wchicago.il.chicago.xyz.net,
PKT_INFRA-LINK-5-CHANGED-sur03.wchicago.il.chicago.xyz.net,
PLATFORM-PLDMGR-4-CLIENT_WARNING-ar01.elmhurst.il.chicago.xyz.net

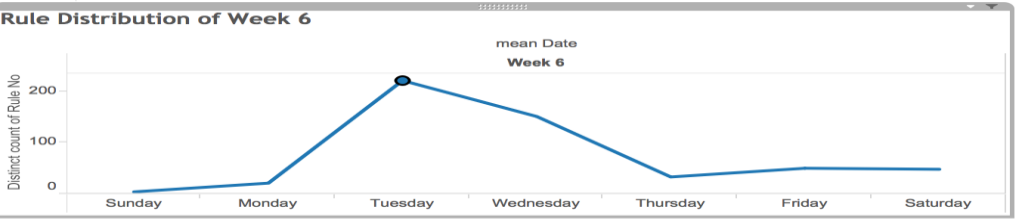
=>

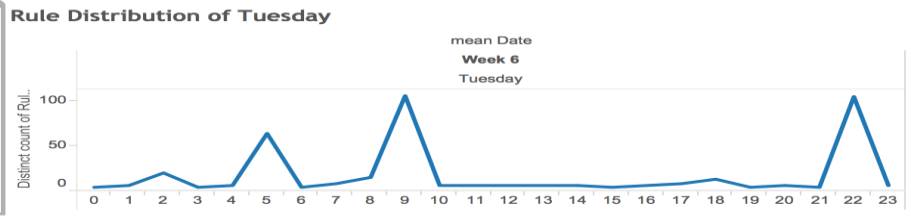
PLATFORM-SFP-3-HIGH_RX_POWER_WARNING
-sur03.wchicago.il.chicago.xyz.net

Rule Patterns

- Below graph shows a regular pattern identified using generated rules – it calls out the occurance of specific rules within maintenance window on every Tuesday morning.
- With the help of developed solution we are able to optimize Millions of syslog messages to few hundred rules and then further to 8-10 very relevant rules
- This can help to focus on relevant rules and ignore unwanted ones.







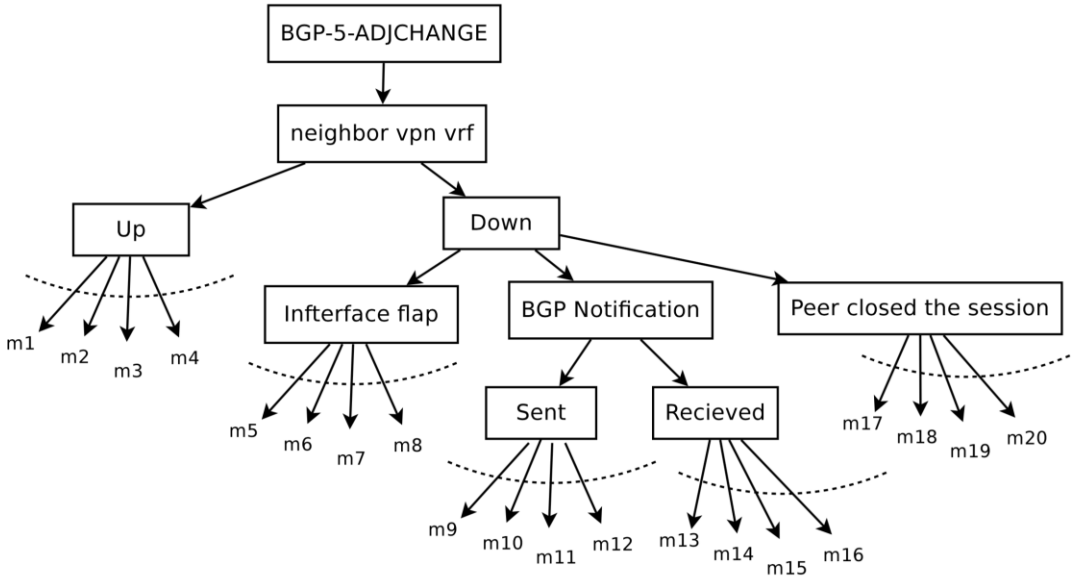
Top 10 Rules of Week 6 Tuesday All

Rule No	Rule	Week of mea..	Weekday of ..	Hour of ..	Numbe..
10	{SECURITY-login-4-AUTHEN_FAILED-ar02-d.mtprospect.il.ndcnort… …RITY-SSHD-3-ERR_GENERAL-ar02-d.mtprospect.il.ndcnor… …UR..	Week 6	Tuesday	22	3
17	{SECURITY-login-4-AUTHEN_FAILED-ar02-d.mtprospect.il.ndcnorth… …ITY-SSHD-3-ERR_GENERAL-ar02-d.mtprospect.il.ndcnor… …UR..	Week 6	Tuesday	22	3
43	{SECURITY-login-4-AUTHEN_FAILED-ar02-d.mtprospect.il.ndcnorth… …ITY-SSHD-3-ERR_GENERAL-ar02-d.mtprospect.il.ndcnor… …UR..	Week 6	Tuesday	9	2
				22	3
61	{SECURITY-login-4-AUTHEN_FAILED-ar02-d.mtprospect.il.ndcnorth… …ITY-SSHD-3-ERR_GENERAL-ar01-d.mtprospect.il.ndcnor… …UR..	Week 6	Tuesday	9	2
100	{SECURITY-login-4-AUTHEN_FAILED-ar02-d.mtprospect.il.ndcnorth… …ITY-SSHD-3-ERR_GENERAL-ar02-d.mtprospect.il.ndcnor… …UR..	Week 6	Tuesday	9	2
106	{SECURITY-login-4-AUTHEN_FAILED-ar02-d.mtprospect.il.ndcnorth… …ITY-SSHD-3-ERR_GENERAL-ar02-d.mtprospect.il.ndcnor… …UR..	Week 6	Tuesday	9	2

Message Template Generation

Below messages belong to same message type
(BGP-5-ADJCHANGE)

m_1	neighbor 192.168.32.42 vpn vrf 1000:1001 Up
m_2	neighbor 192.168.100.194 vpn vrf 1000:1002 Up
m_3	neighbor 192.168.15.78 vpn vrf 1000:1003 Up
m_4	neighbor 192.168.108.38 vpn vrf 1000:1004 Up
m_5	neighbor 192.168.0.26 vpn vrf 1000:1004 Down Interface flap
m_6	neighbor 192.168.7.6 vpn vrf 1000:1001 Down Interface flap
m_7	neighbor 192.168.0.238 vpn vrf 1000:1003 Down Interface flap
m_8	neighbor 192.168.2.114 vpn vrf 1000:1002 Down Interface flap
m_9	neighbor 192.168.183.250 vpn vrf 1000:1002 Down BGP Notification sent
m_{10}	neighbor 192.168.114.178 vpn vrf 1000:1003 Down BGP Notification sent
m_{11}	neighbor 192.168.131.218 vpn vrf 1000:1001 Down BGP Notification sent
m_{12}	neighbor 192.168.55.138 vpn vrf 1000:1000 Down BGP Notification sent
m_{13}	neighbor 192.168.1.13 vpn vrf 1000:1000 Down BGP Notification received
m_{14}	neighbor 192.168.12.241 vpn vrf 1000:1002 Down BGP Notification received
m_{15}	neighbor 192.168.155.66 vpn vrf 1000:1003 Down BGP Notification received
m_{16}	neighbor 192.168.254.29 vpn vrf 1000:1004 Down BGP Notification received
m_{17}	neighbor 192.168.35.230 vpn vrf 1000:1004 Down Peer closed the session
m_{19}	neighbor 192.168.171.166 vpn vrf 1000:1001 Down Peer closed the session
m_{19}	neighbor 192.168.2.237 vpn vrf 1000:1002 Down Peer closed the session
m_{20}	neighbor 192.168.0.154 vpn vrf 1000:1003 Down Peer closed the session

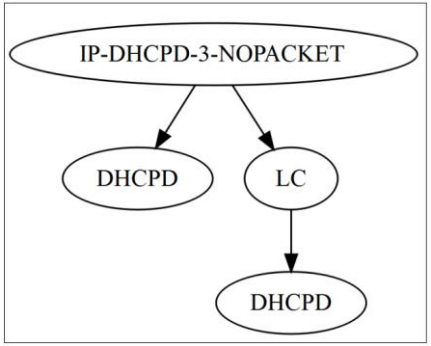


Rule Interpretation (using message template)

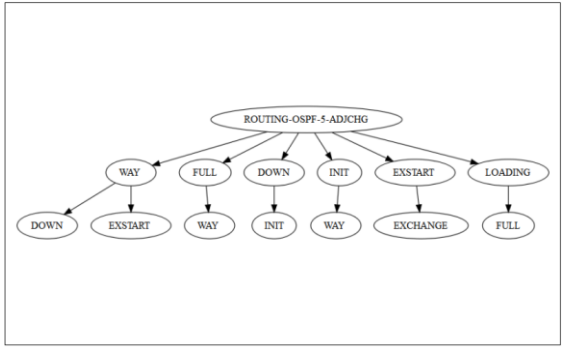
Rule:

IP-DHCPD-3-NOPACKET
ROUTING-OSPF-5-ADJCHG => PLATFORM-SFP-3-HIGH_RX_POWER_WARNING
ROUTING-IPV4_PIM-3-NBRCHG

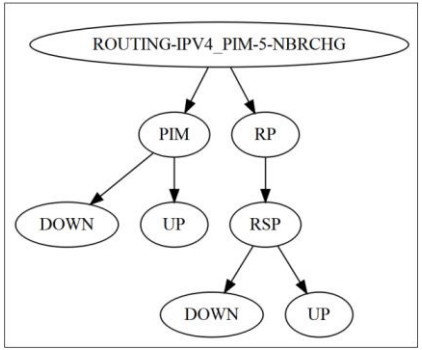
IP-DHCPD-3-NOPACKET



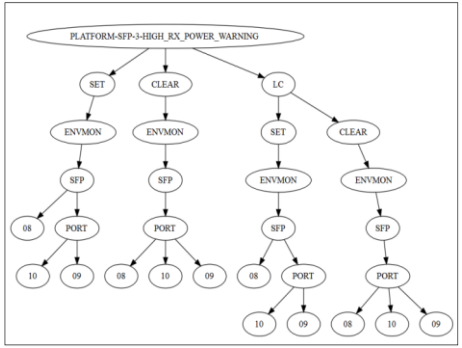
ROUTING-OSPF-5-ADJCHG



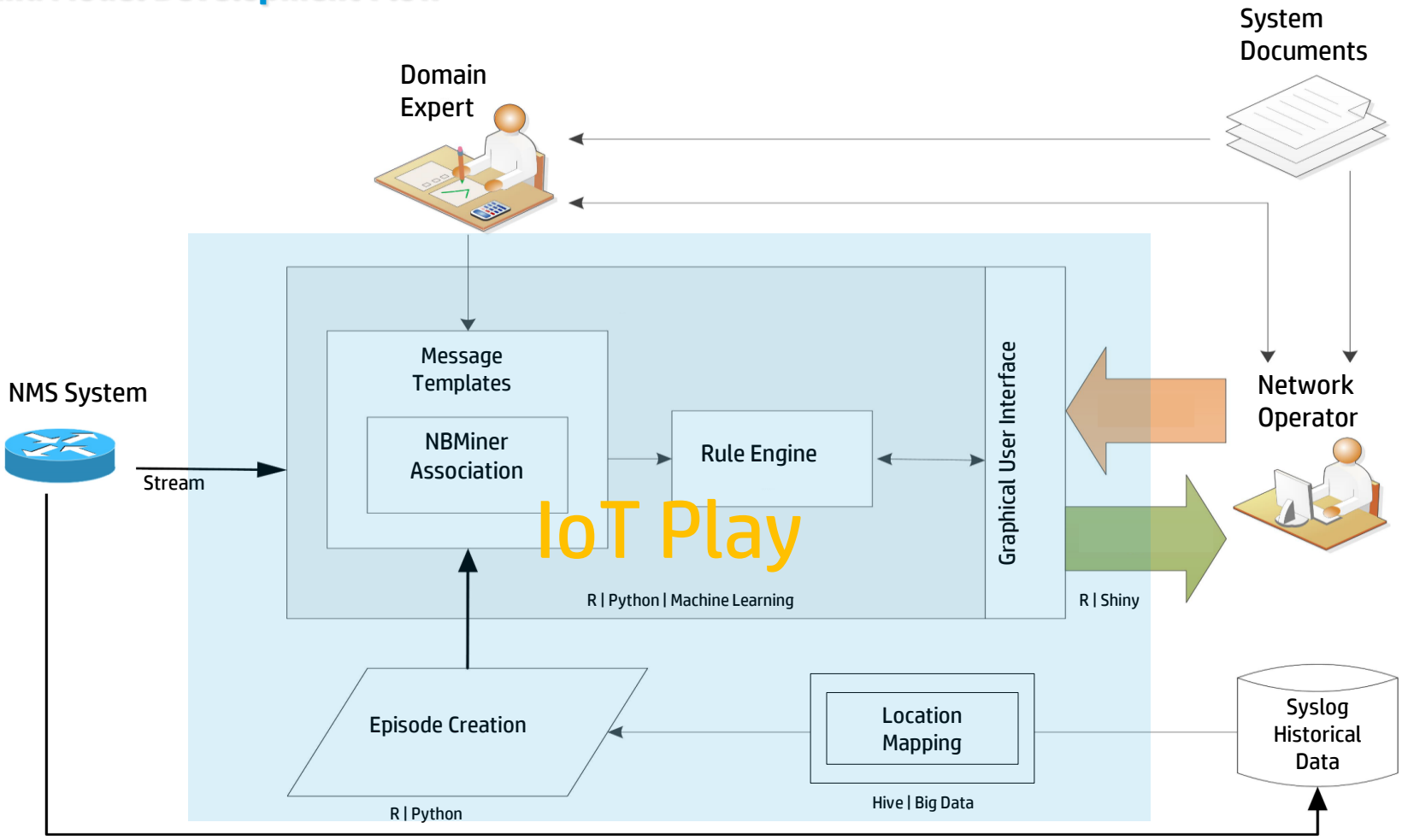
ROUTING-IPV4_PIM-3-NBRCHG



PLATFORM-SFP-3-HIGH_RX_POWER_WARNING



End to End Model Development Flow



Q & A