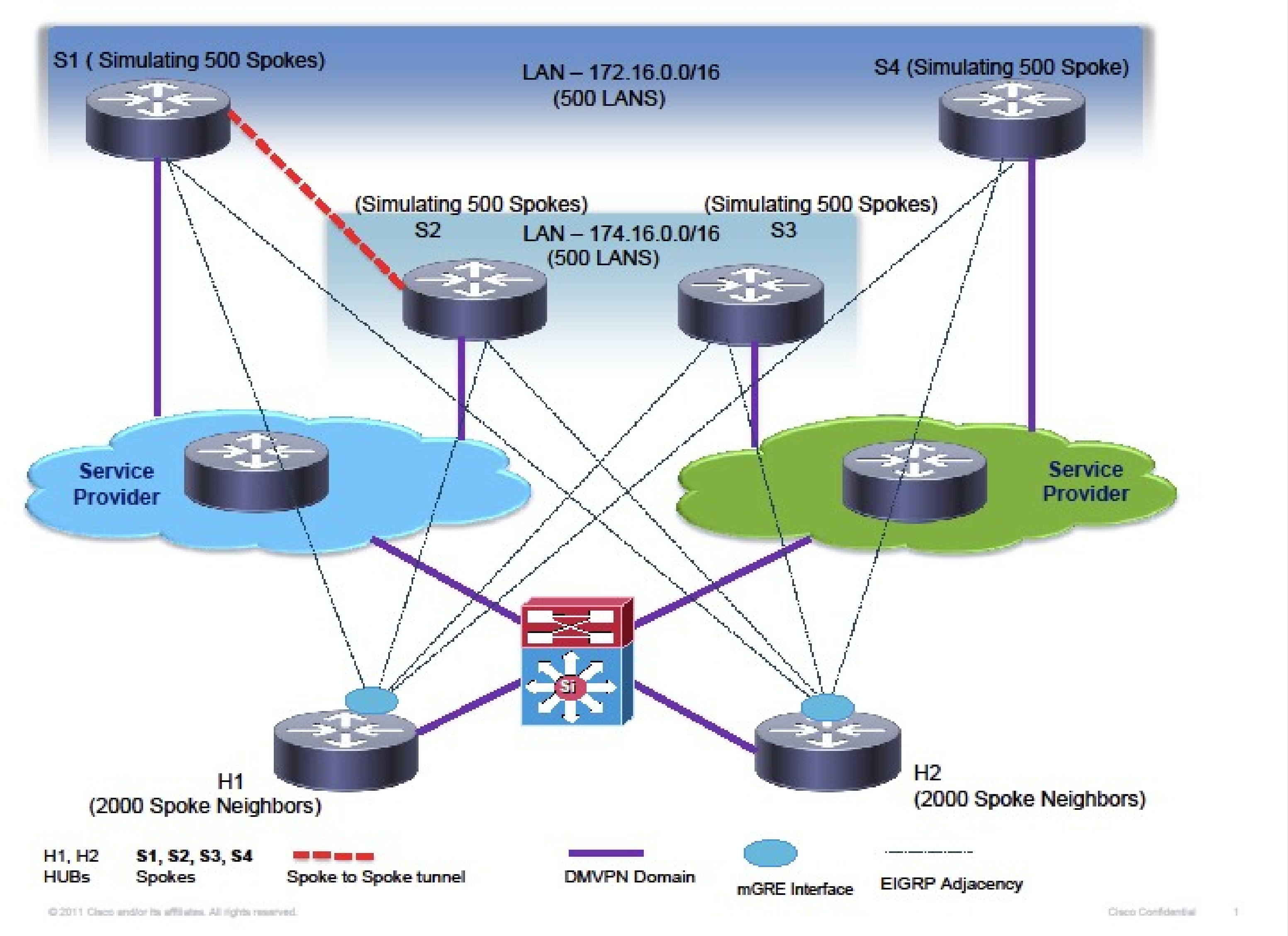
Predicting Interface Failures For Better Traffic Management.

- Rudra Saha
Cisco Systems

28 March 2016

Agenda:

- Problem Scenario
- Current Solution
- Proposed Solution
- Experimental Methodology
- Tasks Done
- Current Outcomes
- Results
- Future Work
- Conclusion
- Q/A


S1 (Simulating 500 Spokes)
LAN – 172.16.0.0/16
(500 LANS)
S4 (Simulating 500 Spoke)
(Simulating 500 Spokes)
S2
LAN – 174.16.0.0/16
(500 LANS)
(Simulating 500 Spokes)
S3
Service Provider
Service Provider
H1
(2000 Spoke Neighbors)
H2
(2000 Spoke Neighbors)
H1, H2
HUBs
S1, S2, S3, S4
Spokes
Spoke to Spoke tunnel
DMVPN Domain
mGRE Interface
EIGRP Adjacency
© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Confidential
1

Current Solution:

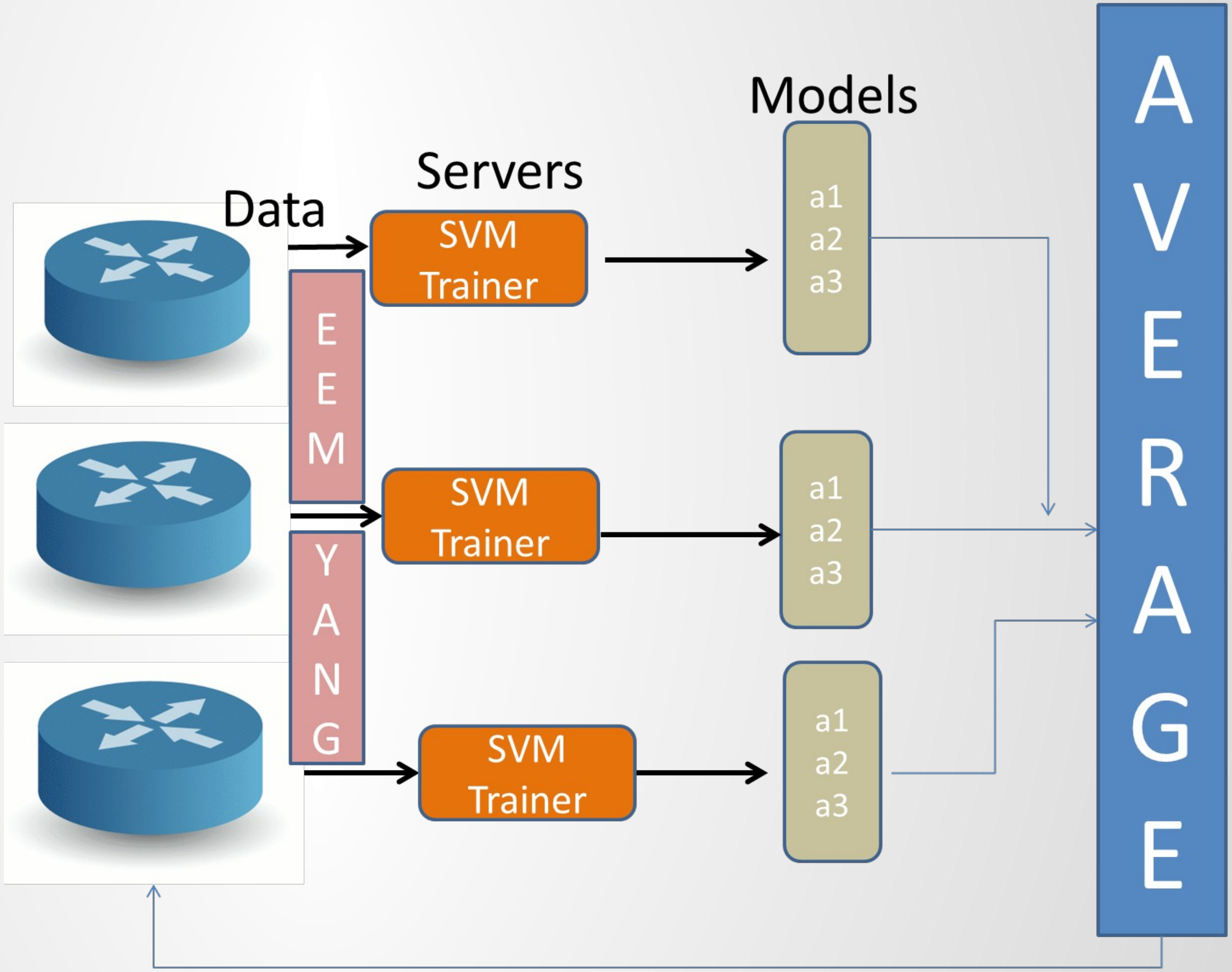
- Essentially reactive in nature.
- Tries to detect and resolve network issues post failure.
- Dependent on redundant paths.
- Doesn’t look into the “Why” of the matter.

28 March 2016

Proposed Solution:

- Pro-active in nature.
- Relies on pattern observed in historical data.
- Minimal affect on router usage while data collection.
- Negligent affect while making prediction outside the router.

Experimental Methodology:



GLOBAL MODEL

28 March 2016

…

- First task is to come up with relevant data.

- EIGRP protocol used because of domain expertise.

- New cli created which collect features from eigrp component.

- Features extracted from the global router level as well

e.g. CPU usage, network bandwidth usage, memory usage etc.

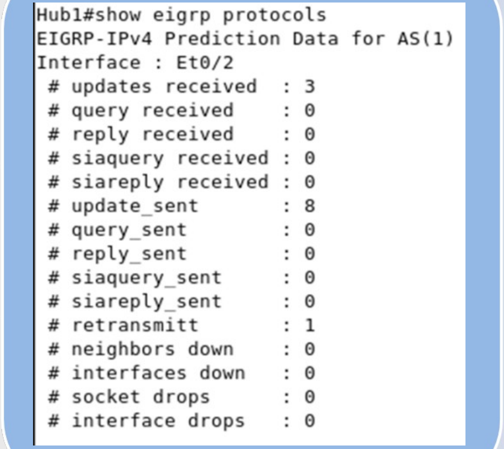
- EEM scripts currently deployed to extract this from the cli.

…

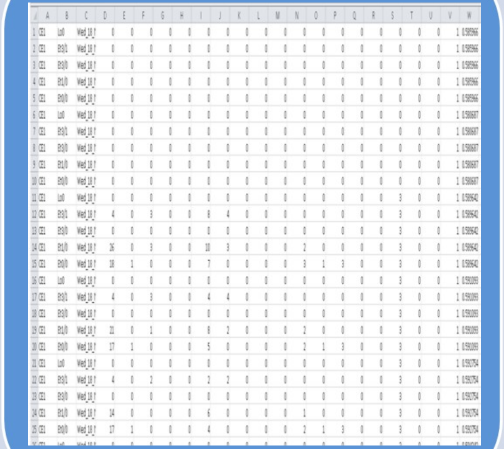
- Data for training and cross-validation purposes collected from a DUAL DMVPN topology with 100 spokes.
- Data is collected in groups of 6 minutes.
- Used One-Class SVM to create our prediction model.
- DBSCAN algorithm used to generate better insights into the data.

...

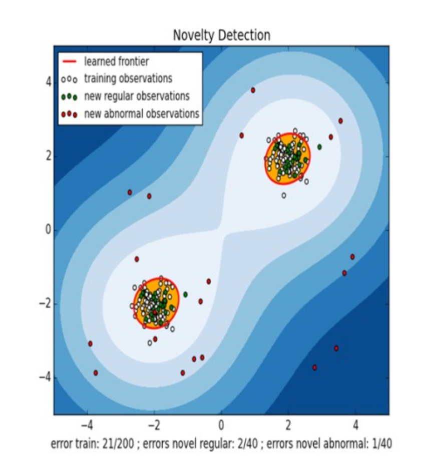
- The events with a route down / CPU hog/ Interface Down/ Traceback/ Crash/ Process Crash etc can be marked as an anomaly.



```
Hub1#show eigrp protocols
EIGRP-IPv4 Prediction Data for AS(1)
Interface : Et0/2
 # updates received   : 3
 # query received     : 0
 # reply received     : 0
 # siaquery received  : 0
 # siareply received  : 0
 # update_sent        : 8
 # query_sent         : 0
 # reply_sent         : 0
 # siaquery_sent      : 0
 # siareply_sent      : 0
 # retransmitt        : 1
 # neighbors down     : 0
 # interfaces down    : 0
 # socket drops       : 0
 # interface drops    : 0
```



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	CE1	Lo0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.585966
2	CE1	Et3/1	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.585966
3	CE1	Et3/0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.585966
4	CE1	Et1/0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.585966
5	CE1	Et0/0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.585966
6	CE1	Lo0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.580687
7	CE1	Et3/1	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.580687
8	CE1	Et3/0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.580687
9	CE1	Et1/0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.580687
10	CE1	Et0/0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0.580687
11	CE1	Lo0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	1	0.589642
12	CE1	Et3/1	Wed_18_f	4	0	3	0	0	8	4	0	0	0	0	0	0	0	0	3	0	0	1	0.589642
13	CE1	Et3/0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	1	0.589642
14	CE1	Et1/0	Wed_18_f	26	0	3	0	0	10	3	0	0	0	2	0	0	0	0	3	0	0	1	0.589642
15	CE1	Et0/0	Wed_18_f	18	1	0	0	0	7	0	0	0	0	3	1	3	0	0	3	0	0	1	0.589642
16	CE1	Lo0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	1	0.591093
17	CE1	Et3/1	Wed_18_f	4	0	3	0	0	4	4	0	0	0	0	0	0	0	0	3	0	0	1	0.591093
18	CE1	Et3/0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	1	0.591093
19	CE1	Et1/0	Wed_18_f	21	0	1	0	0	8	2	0	0	0	2	0	0	0	0	3	0	0	1	0.591093
20	CE1	Et0/0	Wed_18_f	17	1	0	0	0	5	0	0	0	0	2	1	3	0	0	3	0	0	1	0.591093
21	CE1	Lo0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	1	0.592754
22	CE1	Et3/1	Wed_18_f	4	0	2	0	0	2	2	0	0	0	0	0	0	0	0	3	0	0	1	0.592754
23	CE1	Et3/0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	1	0.592754
24	CE1	Et1/0	Wed_18_f	14	0	0	0	0	6	0	0	0	0	1	0	0	0	0	3	0	0	1	0.592754
25	CE1	Et0/0	Wed_18_f	17	1	0	0	0	4	0	0	0	0	2	1	3	0	0	3	0	0	1	0.592754
26	CE1	Lo0	Wed_18_f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	1	[illegible]

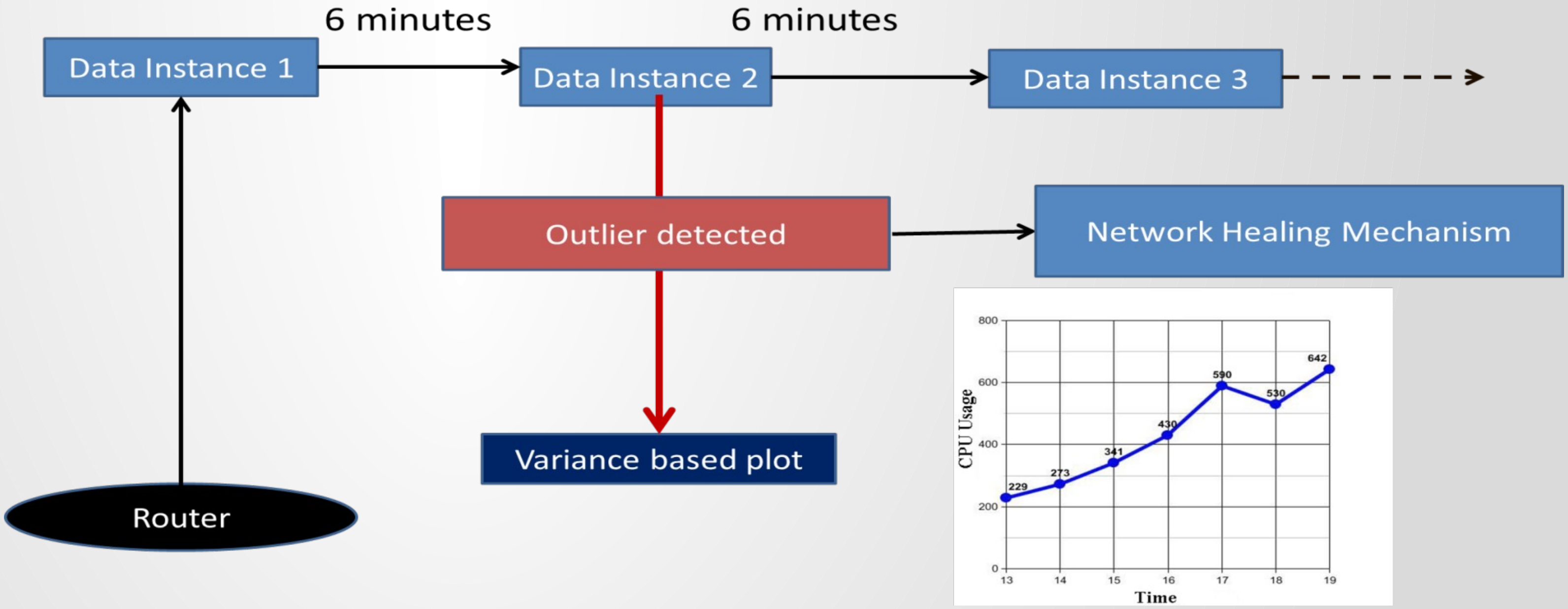


28 March 2016

Current Outcomes:

- Once an outlier is detected, a simple probability model helps us plot the outlier variable vs time

- The prediction will help the admin to switch the traffic to an alternate path at the earliest.



28 March 2016

Results:

- With tailored anomalous data which had continuous high CPU utilization/network drop, the model assessed the nature of the data instance with high certainty.
- Neighbour down due to query storm in the DMVPN network was easily predicted.
- The model was able to predict an EIGRP neighbor flap due to SIA in PE-CE network.
- An accuracy of ~67% was achieved on the test dataset.

Future Work:

- Future work will be to come up with a more robust dataset that covers all the relevant cases.

- Increase upon the number of feature points to improve the model and to come up with different models that suit our data.

- Include features other components from the network stack (lower level) in the prediction model.

- To take corrective action on the router automatically similar to FRR and bypass the issue from happening.

Conclusion:

- We now have a mechanism in place to alert the network admin to take corrective action like diverting traffic from the interface before an issue can happen.

- In case the network admin does not take any preventive action and the failure does happen, the admin will now have a starting point to debug.

how
poll ask challenge poll
problem questions challenge when
what
ask answers investigation who query answers ask
questions confusion
how q&a reply problem puzzle q&a
confusion poll q&a ask what confusion what
asking q&a problem answers interrogation how
puzzle questions reply
query who problem puzzle who problem q&a
ask
poll QUESTIONS challenge
reply
questions questions
what puzzle
q&a investigation interrogation ery investigation ask interrogation
reply ask confusion investig tion q&a query
poll
challenge answers challenge q&a llenge query confusion
query questions investiga quiry problem
when reply how
interrogation who problem
uestions
how puzzle an
what when

28 March 2016