

# *Network Configuration Governance*

*Arkadip Basu*

*LSPE 52<sup>nd</sup> meet up*

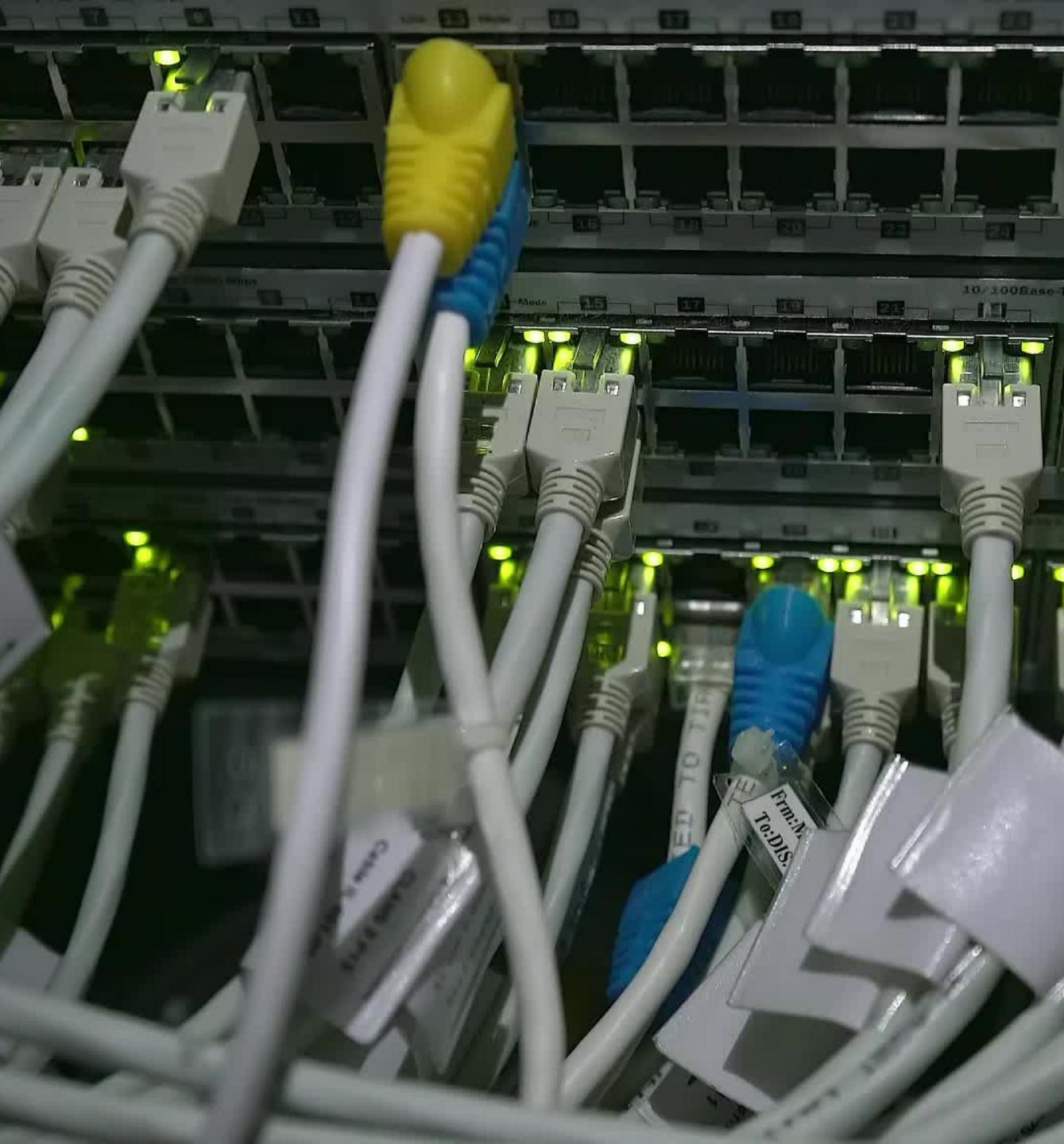
*September 2024, Bangalore*

What is Configuration

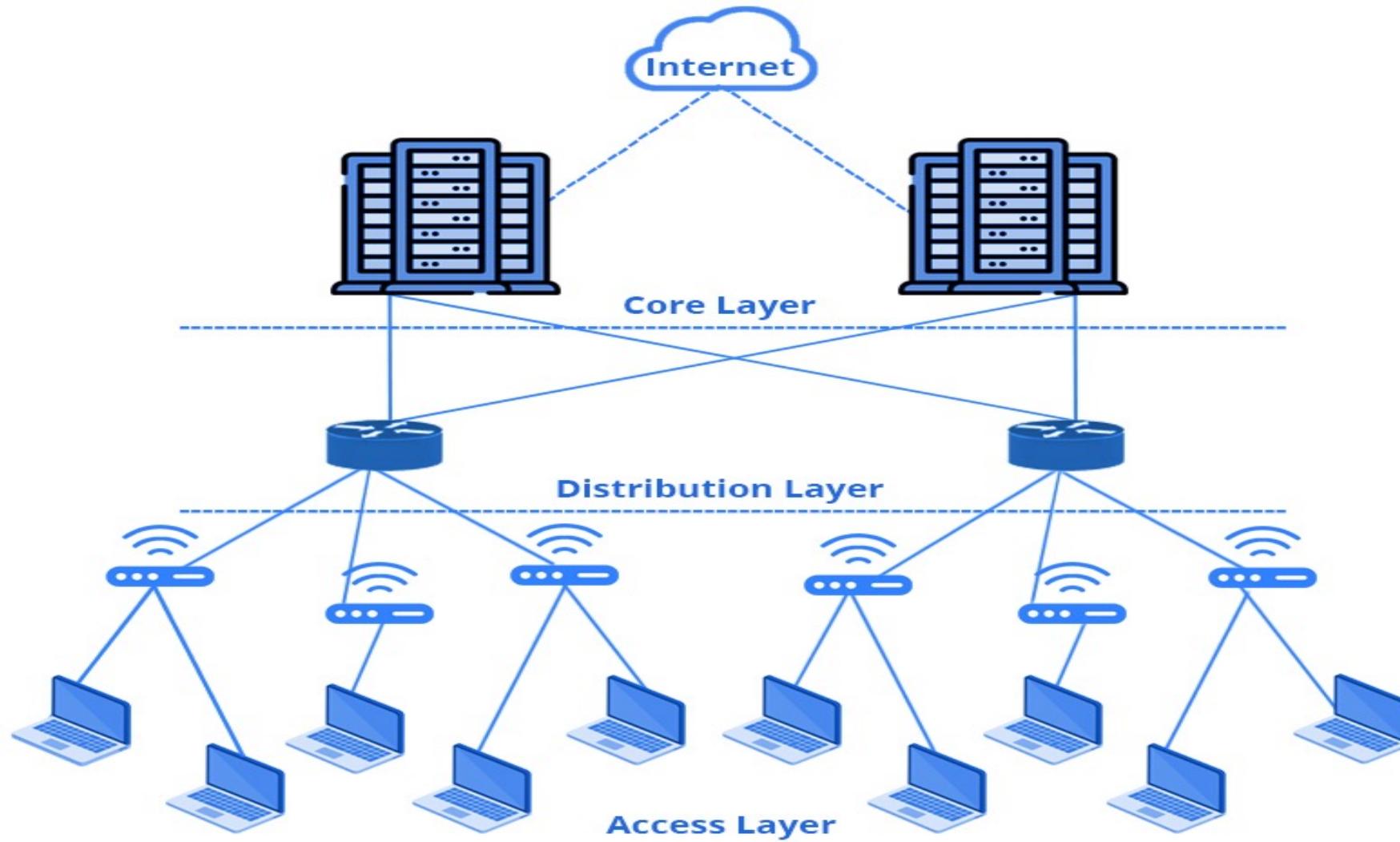
Why it is required

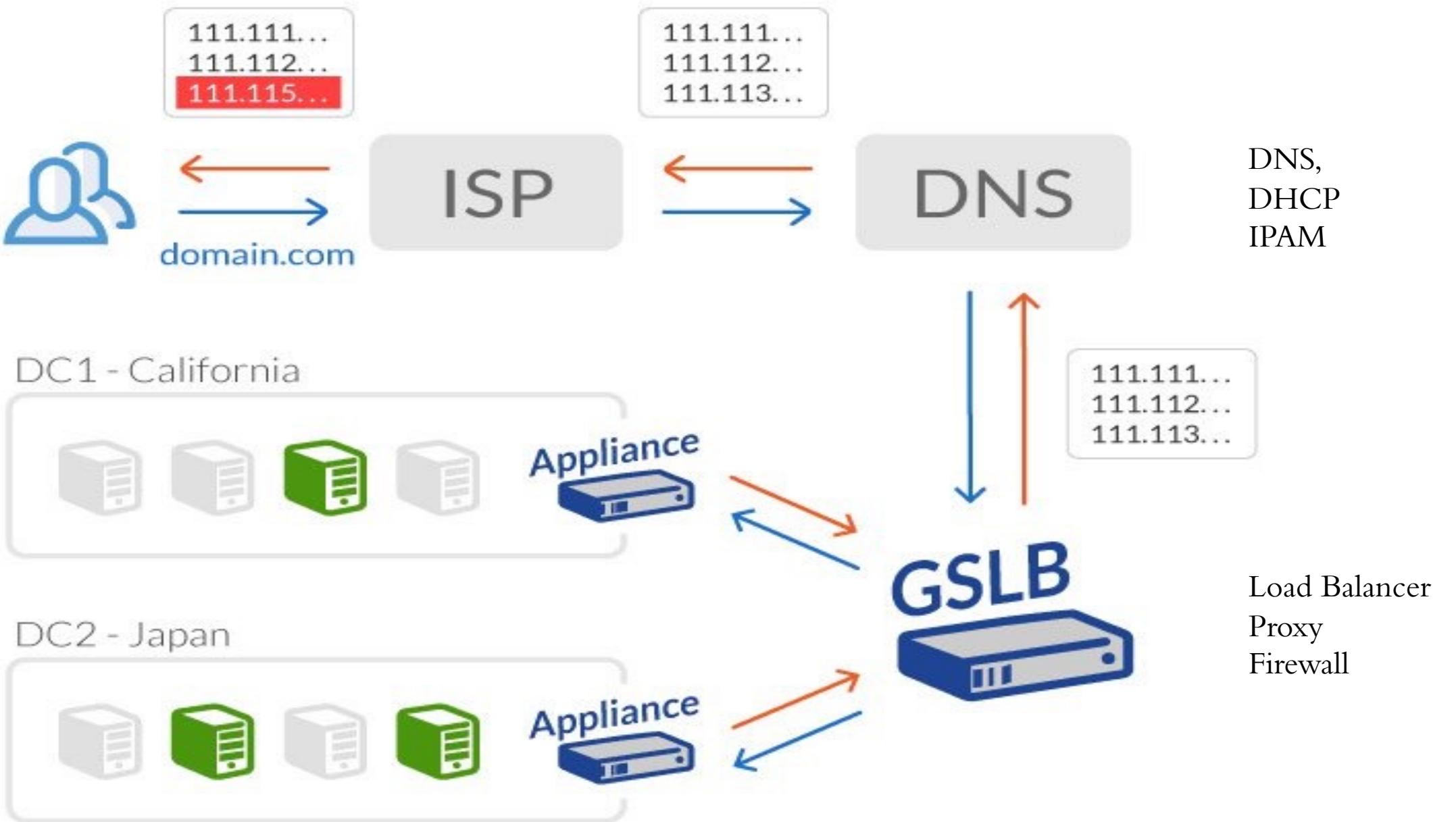
Why that needs to be controlled

*How Good Governance will help  
Business impact*



# *Network Architecture*





```
r-m[1]#gg-1#
r-m[1]#gg-1# sh run

!Command: show running-config
!Running configuration last done at: Tue Jun 11 01:37:24 2024
!Time: Tue Jun 11 02:06:27 2024

version 9.3(10) Bios:version 05.47
hostname r-m[1]gg-1
vdc r-m[1]gg-1 id 1
    limit-resource vlan minimum 16 maximum 4094
    limit-resource vrf minimum 2 maximum 4096
    limit-resource port-channel minimum 0 maximum 511
    limit-resource u4route-mem minimum 248 maximum 248
    limit-resource u6route-mem minimum 96 maximum 96
```

Running Configuration  
of a Network device

```
r-m[1]# -1#
r-m[1]# -1# sh run | in log
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
snmp-server enable traps bridge topologychange
snmp-server enable traps syslog message-generated
aaa authentication login default group PCI_TACACS
    log neighbor changes
logging server 161.17[1] 5 use-vrf management
logging source-interface mgmt0
logging origin-id hostname
r-m[1]#gg-1#
```

Filtering out the log section  
from Running Configuration  
of a Network device

## Trace the configuration changes from the device (network) CLI

```
)  
Wed Jun 26 22:11:47 2024:type=update:id=172 [REDACTED] 122@pts/0:user=netman:cmd=configure terminal ; crypto ca import gnmicert pkcs12 bootflash:/s-  
1.mgt.wal-mart.com.pfx wilson81 (FAILURE)  
Wed Jun 26 22:14:49 2024:type=update:id=17 [REDACTED] 122@pts/0:user=netman:cmd=configure terminal ; crypto ca trustpoint gnmicert (SUCCESS)  
Wed Jun 26 22:14:59 2024:type=update:id=17 [REDACTED] 122@pts/0:user=netman:cmd=configure terminal ; crypto ca import gnmicert pkcs12 bootflash:/s-  
1.mgt.wal-mart.com.pfx 3D41018Azlkq2cvR20a  
fOLv0 (SUCCESS)  
Wed Jun 26 22:15:24 2024:type=update:id=17 [REDACTED] 122@pts/0:user=netman:cmd=configure terminal ; grpc certificate gnmicert (SUCCESS)  
Fri Jun 28 10:14:25 2024:type=update:id=16 [REDACTED] 4.61@pts/1:user=Netman:cmd=configure terminal ; interface loopback555 (REDIRECT)  
Fri Jun 28 10:14:25 2024:type=update:id=16 [REDACTED] 4.61@pts/1:user=netman:cmd=configure terminal ; interface loopback555 (SUCCESS)  
Fri Jun 28 10:14:38 2024:type=update:id=16 [REDACTED] 4.61@pts/1:user=netman:cmd=configure terminal ; no interface loopback555 (REDIRECT)  
Fri Jun 28 10:14:38 2024:type=update:id=16 [REDACTED] 4.61@pts/1:user=netman:cmd=configure terminal ; no interface loopback555 (SUCCESS)  
s-d [REDACTED] eaf10-1#
```

```
s-drf [REDACTED] 10-1# sh accounting log all | grep 'cmd=conf' | last 1  
Fri Jun 28 10:14:38 2024:type=update:id=16 [REDACTED] 61@pts/1:user=netman:cmd=configure terminal ; no interface loopback555 (SUCCESS)  
s-drf [REDACTED] 10-1# sh accounting log all | grep 'cmd=conf' | last 2  
Fri Jun 28 10:14:38 2024:type=update:id=16 [REDACTED] 61@pts/1:user=netman:cmd=configure terminal ; no interface loopback555 (REDIRECT)  
Fri Jun 28 10:14:38 2024:type=update:id=16 [REDACTED] 61@pts/1:user=netman:cmd=configure terminal ; no interface loopback555 (SUCCESS)  
s-drf.srv11eaf10-1# sh accounting log all | grep 'cmd=conf' | last 3
```

# Raw logs as arrived over the configured listener endpoint

index="network\_syslog" "\*Configured from vty by\*" NOT vulnscansvc | rex field=\_raw "\w+\s+d+\s+d+\s+d+\s+DeviceName.\*(\s|)\s+d+.+by\s(?<User>\w+)\son\s(?<sourceIP>.\\*)8" | table \_time DeviceName User sourceIP | dedup DeviceName | rex field=DeviceName "(?<dev>\S+)" | fields - DeviceName | fields \_time dev sourceIP User | rex field=dev "\w+-(<subset>\w+)-.\*"

✓ 35 events [6/11/24 5:42:00.000 AM to 6/11/24 6:42:17.000 AM] No Event Sampling Job ▾

Events (35) Patterns Statistics (11) Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection ▷ Download

Raw ▾ Format 50 Per Page ▾

◀ Hide Fields ▶ All Fields

SELECTED FIELDS

- DeviceName 11
- host 11
- source 11
- sourceIP 4
- sourcetype 1
- User 4

INTERESTING FIELDS

- # date\_hour 2
- # date\_mday 1
- # date\_minute 26
- date\_month 1
- # date\_second 25
- date\_wday 1
- # date\_year 1
- date\_zone 1
- device\_name 7
- deviceUnderTest 1
- DP\_AppName 1
- field1 1
- field10 2
- field11 1
- field12 1
- field13 1

Event

Jun 11 06:40:00 10.224.192.254 r-cdc-s-1: 2024 Jun 11 01:40:00 CDT: %VSHD-5-VSHD\_SYSLOG\_CONFIG\_I: Configured from vty by a0b01hu on 10.9 50pts/0

Event Actions ▾

Type	Field	Value	Actions
Selected	DeviceName	10.224.192.254 r-cdc-s-1	▼
	User	a0b01hu	▼
	host	10.224.192.254	▼
	source	/data/syslog_data/network_syslog.log	▼
	sourceIP	10.224.192.254	▼
	sourcetype	syslog	▼

Event

DP_AppName	11
Log	2024
deviceUnderTest	2024
device_name	r-cdc-s-1
field1	Jun
field10	CDT:
field11	%VSHD-5-VSHD_SYSLOG_CONFIG_I:
field12	Configured
field13	from

# Validation Data

neteng\_splunk\_config\_chg4

Save Save As ▾ View Create Table View Close

```
index="network_syslog" "*Configured from vty by* NOT vulnscansvc  
| rex field=_raw "\w+\s+\d+\s\d+:\d+:\d+\s(?<DeviceName>.*)\s|\):\s\d+.*\by\s(?<User>\w+)\son\s(?<sourceIP>.*@\s  
| table _time DeviceName User sourceIP  
| dedup DeviceName  
| rex field=DeviceName "^(?<dev>\S+)"  
| fields - DeviceName  
| fields _time dev sourceIP User  
| rex field=dev "\w+-(<subset>\w+-)*"  
| eval Time=strftime(_time, "%Y-%m-%d %H:%M UTC")  
| eval format=dev." || ".User." || ".sourceIP. " || ".Time
```

Last 15 minutes ▾



✓ 3 events (6/28/24 9:49:08.000 AM to 6/28/24 10:04:08.000 AM) No Event Sampling ▾

Job ▾ II III A B L Verbose Mode ▾

Events (3) Patterns Statistics (3) Visualization

100 Per Page ▾ / Format Preview ▾

_time	dev	/	sourceIP	/	User	/	Time	/	format	/	subset
2024-06-28 09:57:20	r-edc-	-mart.com	18.22.44	/	netman	/	2024-06-28 09:57 UTC	/	r-edc-	/	44    2024-06-28 09:57 UTC
2024-06-28 09:57:46	s-ndc-	t.wal-mart.com	18.22.44	/	netman	/	2024-06-28 09:57 UTC	/	s-ndc-	/	6.22.44    2024-06-28 09:57 UTC
2024-06-28 09:57:33	r-edc-	t.wal-mart.com	18.22.44	/	netman	/	2024-06-28 09:57 UTC	/	r-edc-	/	6.22.44    2024-06-28 09:57 UTC

# Production Data

Search   Analytics   Datasets   Reports   Alerts   Dashboards   > Search & Reporting

## neteng\_splunk\_config\_chg4\_Clone\_3

Save   Save As ▾   View   Create Table View   Close

```
index="network_syslog" "*Configured from vty by* NOT vulnscansvc | rex field=_raw "\w+\s+\d+\s\d+:\d+:\d+\s(?<DeviceName>.*)(\s|):\s\d+.*by\s(?<User>\w+)\son\s(?<sourceIP>.*)_@\s" | table _time DeviceName User sourceIP | dedup DeviceName | rex field=DeviceName "^(?<dev>\S+)" | fields - DeviceName | fields _time dev sourceIP User | rex field=dev "\w+-(<subset>)\w+-.*"
```

Last 60 minutes

✓ 33 events (6/11/24 5:34:00.000 AM to 6/11/24 6:34:02.000 AM)   No Event Sampling ▾   Job ▾   Verbose Mode ▾

Events (33)   Patterns   **Statistics (11)**   Visualization

100 Per Page ▾   / Format   Preview ▾

_time	dev	sourceIP	User	subset
2024-06-11 05:50:39	r-mcc0	172.16.1.97	m0k0cyv	mcc01
2024-06-11 06:12:21	s-cdc-	10.2.1.44	neteng	cdc
2024-06-11 06:20:27	r-mcc0	172.16.1.97	m0k0cyv	mcc01
2024-06-11 06:14:22	r-cdc-	10.2.1.191	netman	cdc
2024-06-11 05:41:25	r-mcc0	172.16.1.97	m0k0cyv	mcc01
2024-06-11 05:48:11	r-dgtclab	10.2.1.44	netman	dgtclab
2024-06-11 05:48:00	r-dgtclab	10.2.1.44	netman	dgtclab
2024-06-11 06:27:01	s-dgtclab	10.2.1.44	netman	dgtclab
2024-06-11 06:13:06	10.224	10.2.1.44	netman	
2024-06-11 05:52:32	r-mcc0	172.16.1.97	m0k0cyv	mcc01

```
↳ napa_api_example_4.py > run_based_on_user_device
191 def run_based_on_user_device():
192     job_client = JobAPIWrapper('svc_accounting', os.environ['svc_accounting_password'], napa_e > c
193     # config = "sh run | head lines 3 | last 1"
194     config = "show accounting log all | in ':cmd=configure terminal ;' | last 1"
195     res = job_client.get_deviceid_result(device_name)
196     if res.json()["count"] >= 1:
197         dev_id = res.json()["results"][0]["url"].split("devices")[1]
198         deviceid = dev_id.replace('/', '')
199         print("deviceid: ", deviceid)
200     else:
201         print("This device is not available.")
202         exit(0)
203     res = job_client.create_new_job("RPOJOB-" + str(timestr), "device", int(deviceid), 3, 0
204     if res is None:
205         print("job creation failed!")
206     else:
207         # print("json result: {}".format(res.json())) # uncomment during debug
208         # print("error: {}".format(res.json()["error"])) # uncomment during debug
209         print("job creation successful")
210     # print("=====\\n\\n")
```

PROBLEMS ① OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS

```
(napa) NAPA_API_EXAMPLE|main> -
(napa) NAPA_API_EXAMPLE|main> - python napa_api_example_4.py
20240628-153859
Enter the device_host_name: s-drf-[REDACTED]
  % Total    % Received % Xferd  Average Speed   Time   Time   Time  Current
          Dload  Upload Total Spent   Spent    Left  Speed
100  174  100  174    0     0   122      0:00:01  0:00:01 ---:---  122
s-drf-[REDACTED]-1
s-drf-[REDACTED]2-1.mgt.wal-mart.com.
10.[REDACTED].28
cisco
nx-os
Operated device : s-drf-[REDACTED]-1.mgt.wal-mart.com.
deviceid: 1620
job creation successful
Ignition on..
```

## default

GET /check-health Health

POST /test\_governance Test

network device config change notification is coming from MLS alert

### Parameters

[Cancel](#)

[Reset](#)

No parameters

### Request body required

application/json

```
{  
    "app": "search",  
    "owner": "a0b01hu",  
    "result": {  
        "User": "m0k0cyv",  
        "time": "1718086164",  
        "dev": "r-mcc01.walmart.com",  
        "sourceIP": "172.17.0.97",  
        "subset": "mcc01"  
    },  
    "results_link": "https://mls-gtp.prod.walmart.com/app/search/search?q=%7Cloadjob%20scheduler_a0b01hu_search_RMD5747500ced2c4cddb_at_1718087400_61043_BC3658C1-1CBD-4608-A5DB-D8505DC7059C%20%7C%20head%205%20%7C%20tail%201&earliest=0&latest=now",  
    "search_name": "neteng_splunk_config_chg4",  
    "sid": "scheduler_a0b01hu_search_RMD5747500ced2c4cddb_at_1718087400_61043_BC3658C1-1CBD-4608-A5DB-D8505DC7059C"  
}
```

```
○ (napa) NAPA_API_EXAMPLE|main> ==
○ (napa) NAPA_API_EXAMPLE|main> == python3 fastapi_webhook_2.py
INFO:     Started server process [59520]
INFO:     Waiting for application startup.
INFO:     Application startup complete.
INFO:     Uvicorn running on http://127.0.0.1:8000 (Press CTRL+C to quit)
@000 11-06-2024 11:22      11-06-2024 12:02      r-mcc01-ecx1agg-2
1 Record inserted successfully into public.test_conf_chg_notification table

*****
{'User': 'm0k0cyv', '_time': '17180085152', 'dev': 'r-mcc01-ecx1agg-1.mgt.wal-mart.com', 'sourceIP': '172.16.1.97', 'subset': 'mcc01'}
*****
INFO: 127.0.0.1:59049 - "POST /test_governance HTTP/1.1" 200 OK

=====
@000 11-06-2024 11:39      11-06-2024 12:14      r-mcc01-ecx1agg-1
1 Record inserted successfully into public.test_conf_chg_notification table

*****
{'User': 'm0k0cyv', '_time': '17180086164', 'dev': 'r-mcc01-ecx1agg-1.mgt.wal-mart.com', 'sourceIP': '172.16.1.97', 'subset': 'mcc01'}
*****
@000 28-06-2024 09:57      28-06-2024 09:00:06
1 Record inserted successfully into public.test_conf_chg_notification table
$$$$ test api slack msg {'validation_type': 'Network Governance', 'data': '{\n    "User": "netman",\n    "_time": "1719568666",\n    "dev": "s-ndc01-ecx1agg-1.mgt.wal-mart.com",\n    "sourceIP": "10.22.22.44",\n    "subset": "ndc"\n}'}
*****
{'_time': '1719568666', 'dev': 's-ndc01-ecx1agg-1.mgt.wal-mart.com', 'sourceIP': '10.22.22.44', 'User': 'netman', 'subset': 'ndc'}
*****
INFO: 10.5.195.81:37420 - "POST /test_governance HTTP/1.1" 200 OK
@000 28-06-2024 09:28      28-06-2024 10:00:07
1 Record inserted successfully into public.test_conf_chg_notification table
$$$$ test api slack msg {'validation_type': 'Network Governance', 'data': '{\n    "User": "admin",\n    "_time": "1719566881",\n    "dev": "r-cndc01-ecx1agg-1.mgt.wal-mart.com",\n    "sourceIP": "10.22.22.3.7",\n    "subset": "cndc1ctaland"\n}'}
*****
{'_time': '1719566881', 'dev': 'r-cndc01-ecx1agg-1.mgt.wal-mart.com', 'sourceIP': '10.22.22.3.7', 'User': 'admin', 'subset': 'cndc1ctaland'}
*****
```

# User Notification

# neteng\_onms\_test ▾ slack channel for testing purpose

+ Add a bookmark

result : 1

"User": "neteng",

Show more

12:00

```
{  
    "app": "search",  
    "owner": "a0b01hu",  
    "result": {  
        "User": "netman",  
        "_time": "1718086386",  
        "dev": "r-cdc-[REDACTED]0.net.wal-mart.com",   
        "sourceIP": "10.[REDACTED].244",  
        "subset": "cdc"  
    },  
    "results_link": "https://mls-gtp.prod.walmart.com/app/search/search?  
q=%7Cloadjob%20scheduler_a0b01hu_search_RMD5747500ced2c4cddb_at_1718  
087400_61043_BC3658C1-1CBD-4608-A5DB-  
D8505DC7059C%20%7C%20head%2010%20%7C%20tail%201&earliest=0&latest=n  
ow",  
    "search_name": "neteng_splunk_config_chg4",  
    "sid":  
    "scheduler_a0b01hu_search_RMD5747500ced2c4cddb_at_1718087400_61043_B  
C3658C1-1CBD-4608-A5DB-D8505DC7059C"  
}
```

Show less

```
{  
    "app": "search",  
    "owner": "a0b01hu",  
    "result": {  
        "User": "m0k0cyv",  
    }  
}
```

Today ▾

# mls\_neteng\_config\_notification ▾ Network\_Device || User || Source\_IP || Time (UTC)

+ Add a bookmark

r-crw-[REDACTED]neoffice.cr.wal-mart.com || vn554xp || 10.78.158.158 || 2024-06-27 Today

r-gtw-[REDACTED]neoffice.gt.wal-mart.com || vn554xp || 10.78.158.158 || 2024-06-27 23:26 UTC

 **Network Governor** APP 5:15 AM

r-crw-[REDACTED]ce.cr.wal-mart.com || vn55wbw || 10.78.193.193 || 2024-06-27 23:33 UTC

r-gtw-[REDACTED]ce.gt.wal-mart.com || jjquint || 10.78.21.21 || 2024-06-27 23:34 UTC

 **Network Governor** APP 5:45 AM

r-gtw-[REDACTED]neoffice.gt.wal-mart.com || jjquint || 10.78.21.21 || 2024-06-28 00:02 UTC

 **Surya Prakash** 8:17 AM

was added to #mls\_neteng\_config\_notification by Arkadip Basu. Also, Ajish Babu joined.

 **Network Governor** APP 10:30 AM

r-dfw-[REDACTED]1.mgt.wal-mart.com || netman || 10.78.44.44 || 2024-06-28 04:46 UTC

 **Network Governor** APP 12:45 PM

r-cdc-v-[REDACTED]gt.wal-mart.com || netman || 161.178.1.1 || 2024-06-28 07:02 UTC

 **Sasikumar Bathiran** 1:14 PM

was added to #mls\_neteng\_config\_notification by Vigneshwaran Lingamani.

 **Network Governor** APP 1:30 PM

r-cdc-v-[REDACTED]gt.wal-mart.com || netman || 161.178.4.61 || 2024-06-28 07:51 UTC

 **Network Governor** APP 2:45 PM

r-cndc1-[REDACTED]cn.wal-mart.com || admin || 10.14.132.132 || 2024-06-28 09:09 UTC

 **Network Governor** APP 3:00 PM

r-cndc1-[REDACTED]wal-mart.com || nettitansvc || 10.14.37.232 || 2024-06-28 09:29 UTC

 **Network Governor** APP 3:30 PM

r-cndc1-[REDACTED]wal-mart.com || admin || 10.14.37.232 || 2024-06-28 09:28 UTC

 **Network Governor** APP 3:30 PM

r-edc-srv-[REDACTED]al-mart.com || netman || 10.22.144.144 || 2024-06-28 09:57 UTC

 **Network Governor** APP 3:30 PM

r-edc-srv-[REDACTED]ngt.wal-mart.com || netman || 10.22.144.144 || 2024-06-28 09:57 UTC

 **Network Governor** APP 3:30 PM

s-ndc-srv-[REDACTED]mgt.wal-mart.com || netman || 10.22.144.144 || 2024-06-28 09:57 UTC

```
[a0b01hu@oser501844 (PROD-CDC) ~/snow_api]$  
[a0b01hu@oser501844 (PROD-CDC) ~/snow_api]$ dzdo python3 snow_api_working.py  
* * * block-2 * *  
  
CHG_Number : CHG2560288  
Short_description : Prod | EDC | Disable NXAPI on Switches  
Planned_start : 05-15-2024 00:00:00  
Planned_end : 05-15-2024 01:59:59  
CHG_State : Closed  
approval_status : Approved  
user_defined_priority : 4 - Low  
user_defined_impact : 4 - Minor  
system_defined_risk : High  
Apm_id : N/A  
cmdb_ci : s-edc-f_____j35-1  
ci_class_name : IP Switch  
Opened_by : Vishal Shivananda (v0s0074)  
assigned_to : Vishal Shivananda (v0s0074)  
assignment_group : GTP-Data Center Network Engineering  
closed_by : Ankit Bhardwaj (a0b0hos)  
    Change has been completed successfully  
    Change has been completed successfully  
Record_url : https://walmartglobal.service-now.com/change_request.do?sys_id=caf3746474e465c51a2  
query=active=true  
[a0b01hu@oser501844 (PROD-CDC) ~/snow_api]$
```

```
* * * getting job real run results. * * *  
"Wed Jun 26 22:15:24 2024:type=update:id=172. [REDACTED]22@pts/0:user=netman:cmd=configure terminal ; grpc certificate gnmicert (SUCCESS)\n\nns-d [REDACTED]f10-1#"  
  
script_result >> Wed Jun 26 22:15:24 2024:type=update:id=172. [REDACTED]22@pts/0:user=netman:cmd=configure terminal ; grpc certificate gnmicert (SUCCESS)\n\n[REDACTED]  
[REDACTED]  
I  
  
network_device_log_date_stamp : Wed Jun 26 22 15 grpc certificate gnmicert  
host_system_date_stamp : Fri Jun 28 15  
No change detected for Today
```



arkadip.basu@walmart.com  
To: Arkadip Basu

Tue 11-Jun-24 10:10 AM

Hi,  
How are you?  
Refer [Splunk](#) for more insights

Where	When	Who	What	Why	Window_Complaint
r-cdc-walmart.com	10-June-2024 11:00AM UTC	a0b01hu	interface loopback 100	CHG123	No
s-edc-walmart.com	10-June-2024 11:23AM UTC	a0b01hu	interface loopback 200	CHG124	No

```
1# vdc s-dfw [REDACTED] c1-1 id 1
2limit-resource vlan minimum 16 maximum 4094
3limit-resource vrf minimum 2 maximum 4096
4 limit-resource port-channel minimum 0 maximum 511
5 limit-resource u4route-mem minimum 248 maximum 248
6limit-resource vrf minimum 2 maximum 4096
7 limit-resource port-channel minimum 0 maximum 511
8 limit-resource u6route-mem minimum 96 maximum 96
9 limit-resource m4route-mem minimum 58 maximum 58
10 limit-resource m6route-mem minimum 8 maximum 8
11
12feature scp-server
13feature tacacs+
14cfs eth distribute
15feature udld
16feature interface-vlan
17feature hsrp
18feature lacp
19feature dhcp
20feature vpc
```

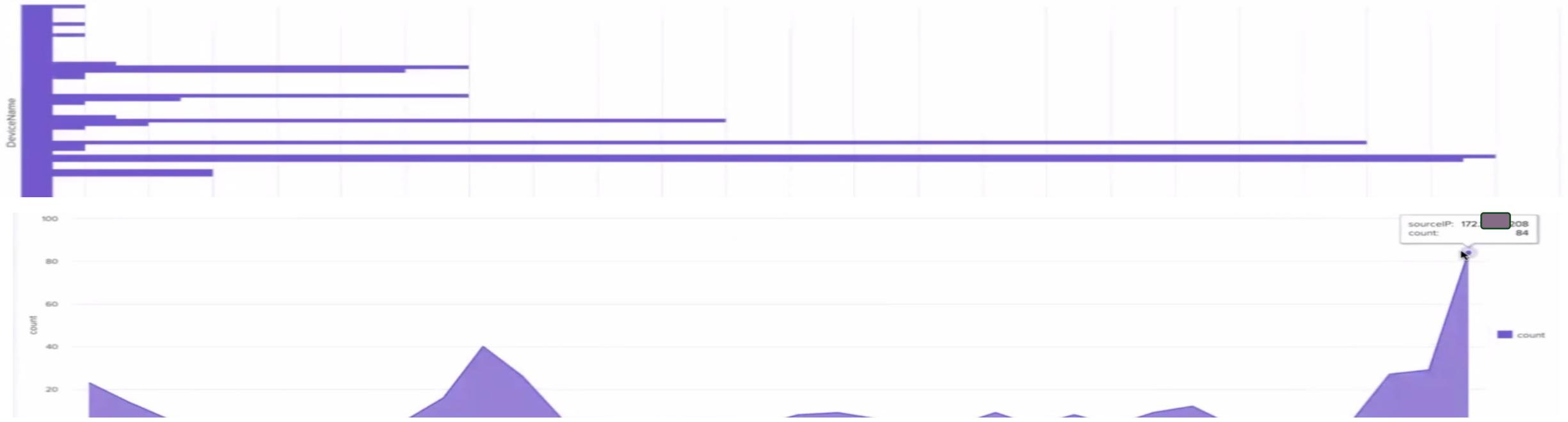
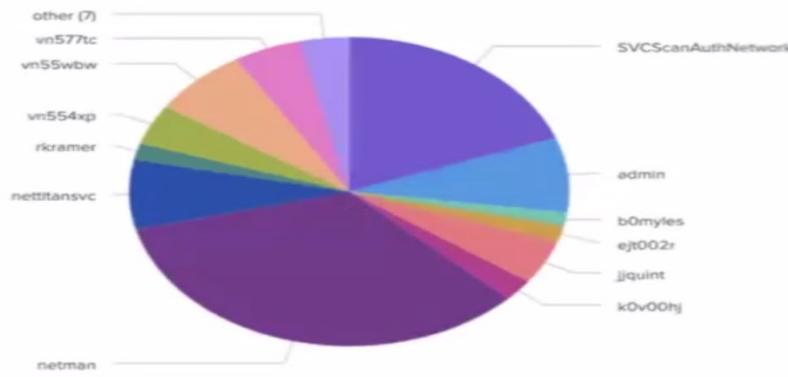
```
1# vdc s-dfw [REDACTED] c1-1 id 1
2limit-resource vlan minimum  maximum 4044
3
4 limit-resource u4route-mem minimum 248 maximum 248
5 limit-resource u6route-mem minimum 96 maximum 96
6 limit-resource m4route-mem minimum 58 maximum 58
7 limit-resource m6route-mem minimum 8 maximum 8
8\ scp-server
9feature tacacs+
10cfs eth distribute
11feature udld
12feature interface-vlan
13feature hsrp
14feature lacp
15feature dhcp
16feature vpc
```

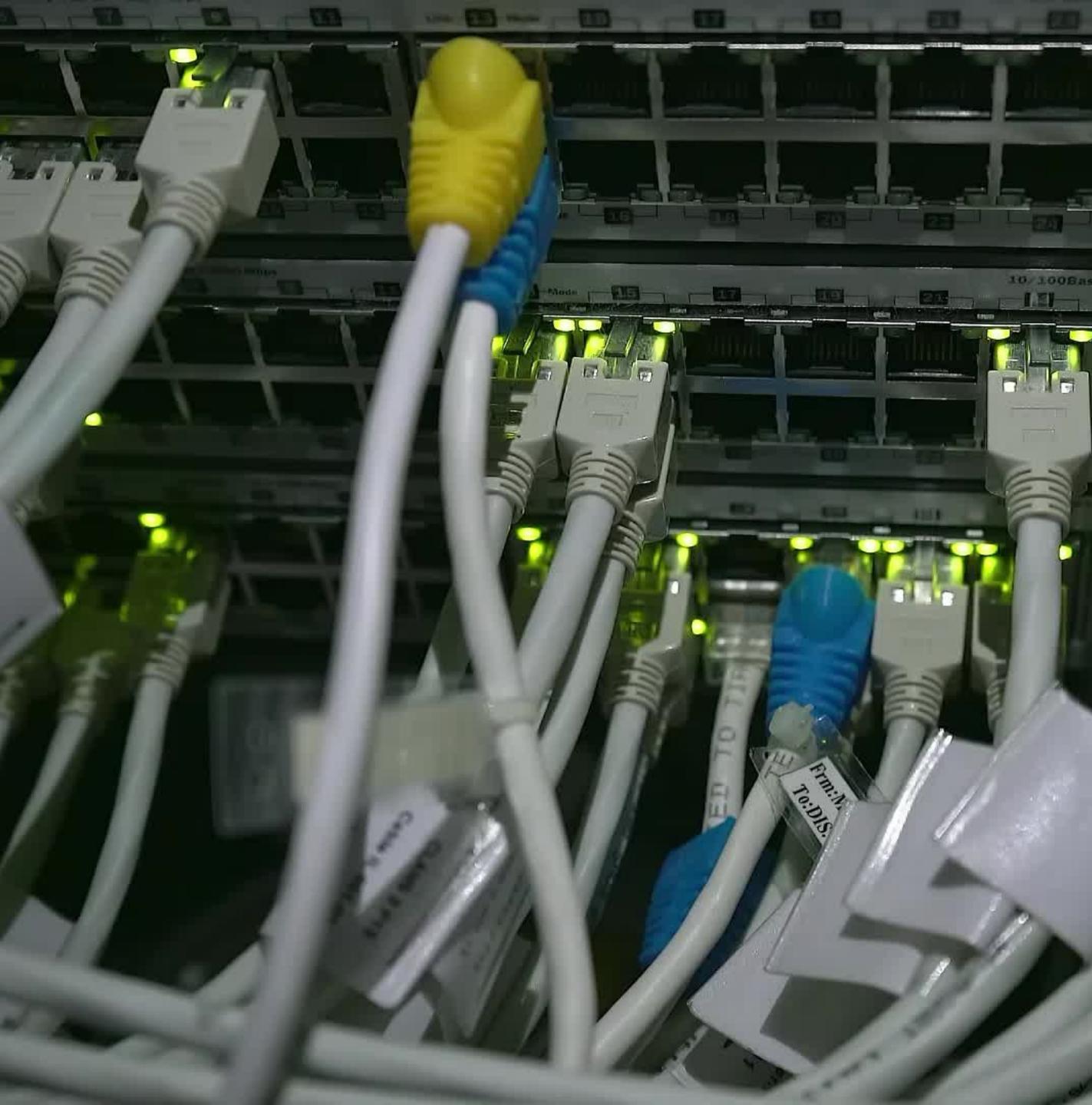
## Network Config Changes

L ▾ Action

Global Time Range

Week to date ▾





## *Questions & Suggestions*

Thank you  
Regards,

Arkadip Basu  
<https://arkadipbasu.github.io>