SNMP

- simple network mgmt. protocol.
- protocol for communicating MIB (Msg Information Base).
- SNMP periodically polls / queries SNMP devices to gather & analyze statistics.
- In normal case, via a GET msg but if a problem occurs, agents will send SNMP TRAP.

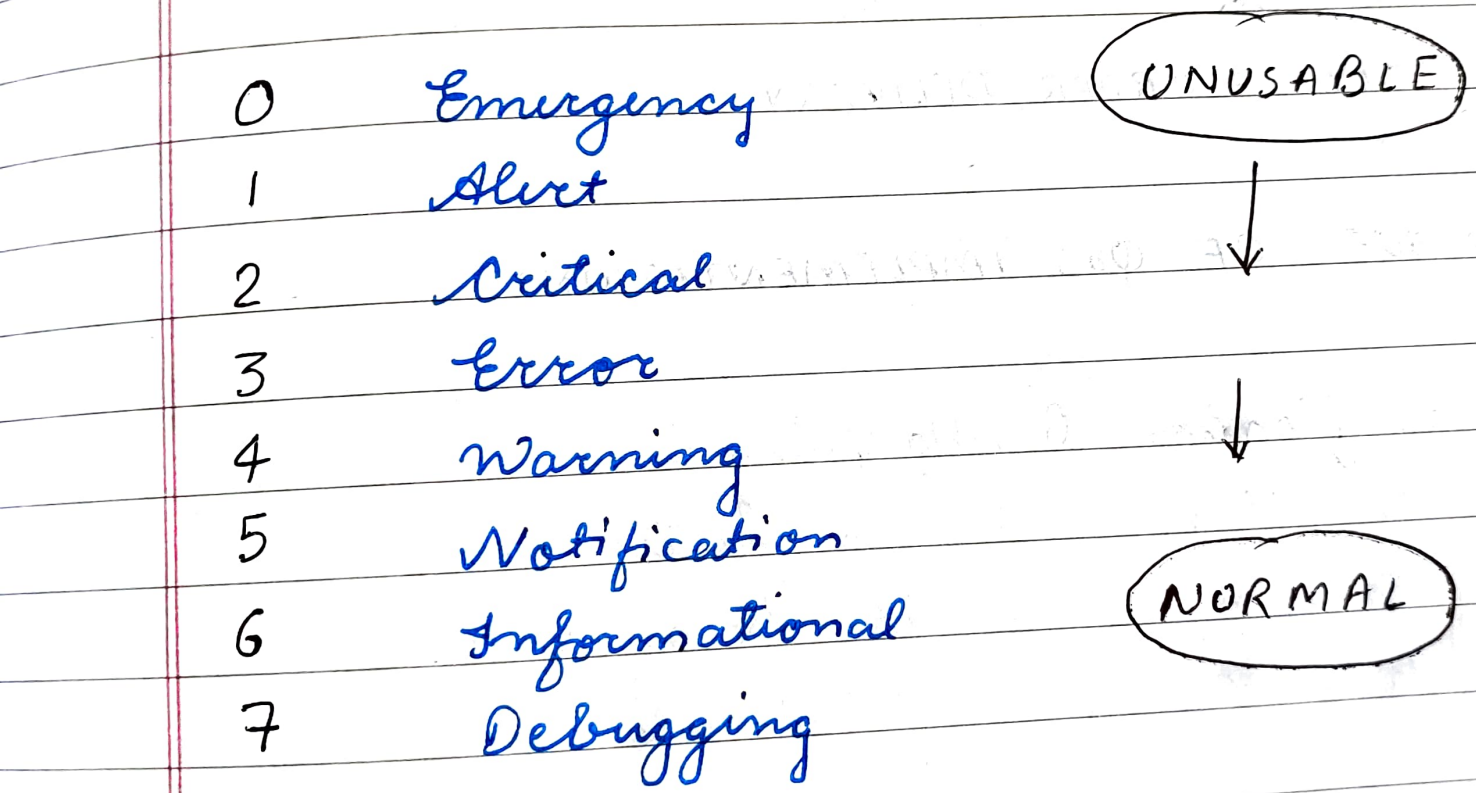
VERSION
- v1 → only UDP, plaintext
- v2c → introduced GET BULK
- v3 → security, confidentiality

MIB: collection of information can be accessed by SNMP like protocols.

GET: MIB to SNMP Manager
SET: SNMP Agent to MIB
WALK: info of successful MIB objects.
TRAP: Error
INFORM: TRAP with Ack.

— — —

PRI SEVERITY LEVELS



← - -

EACEWNID

QoS Quality of Service

QoS focus on following problem:

DELAY

DROPPED PACKETS

ERROR

JITTER

OUT OF ORDER DELIVERY

TECHNIQUES OF QoS IMPLEMENTATION:

(1) Classification & Marking:

- In this, QoS can determine which traffic class it belongs to.
- how the packet should be treated.

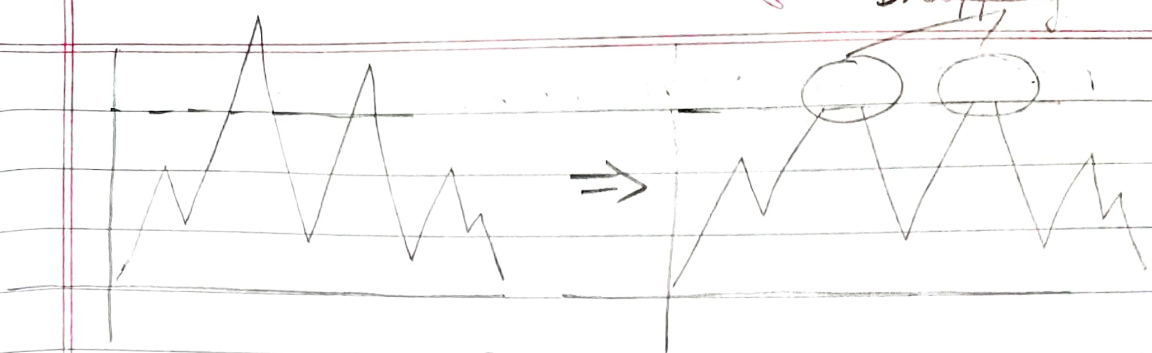
3 BITS (A) CoS: Marking in L2 header

8 BITS (B) ToS: Marking in IPV4 header.

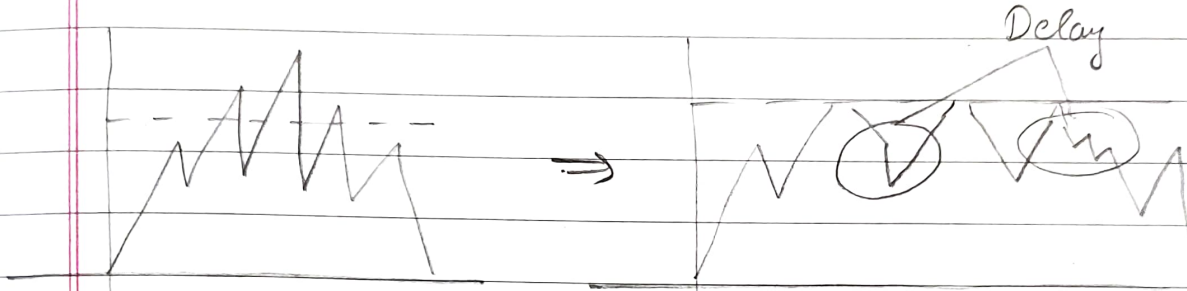
6 BITS (C) DSCP: mordin IP networks

(2) Policing & Shaping: (LLQ)

- Policers drops excess traffic while shapers delay it.
- Both sets a limit on consumption of certain types of data.



POLICING



SHAPING

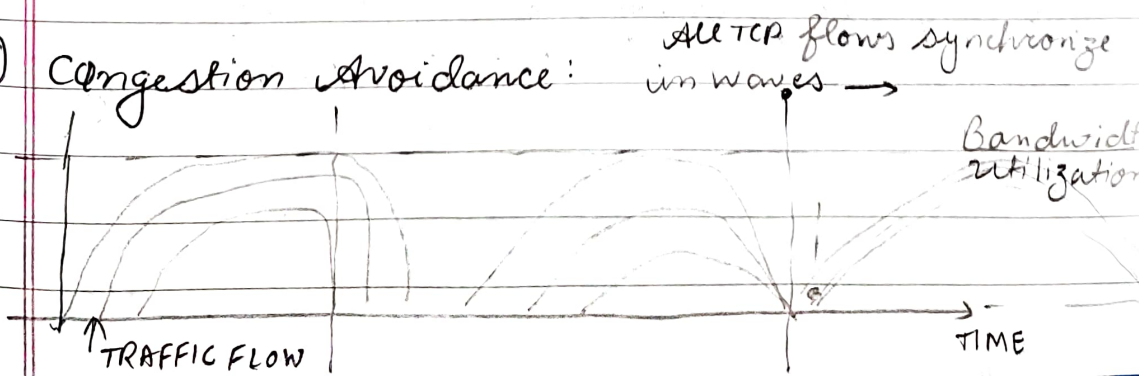
③ Queuing :

- Queuing or Bufferring is the logic of ordering packets in output buffers & it only activated when congestion occurs.

- Scheduling is the step where the decision takes place that which packet should be sent out next.

FIFO , PRIORITY , RR , etc. __

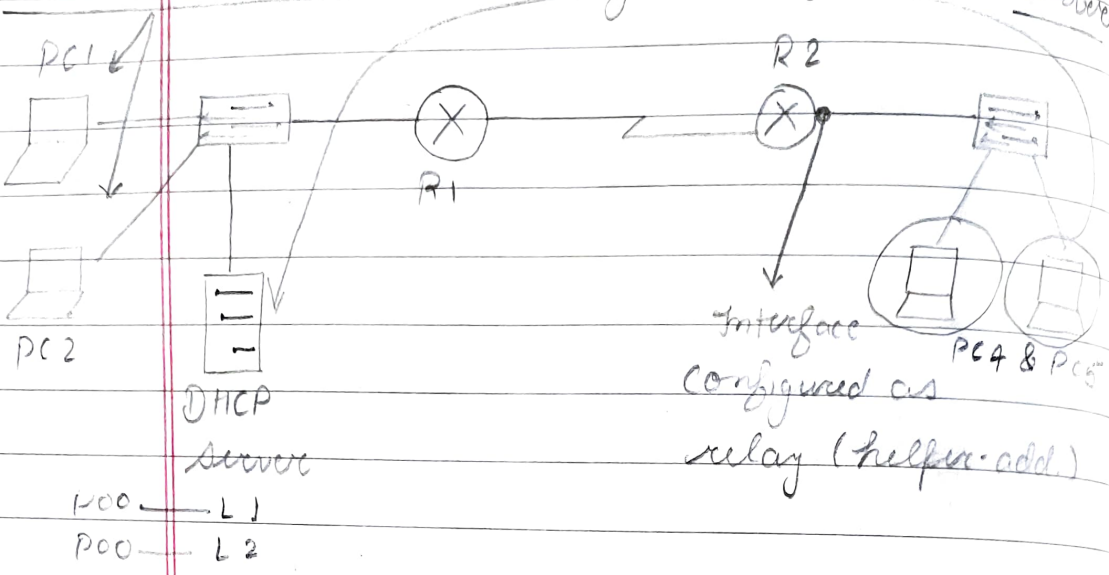
④ Congestion Avoidance :



DHCP SERVER CLIENT RELAY

PC1 & PC2 are DHCP Clients

PC4 & 5 gets add from DHCP Server



P00 — L1
P00 — L2

DHCP SNOOPING : Security implementation to restrict Rogue DHCP server. add 'trusted' ports.

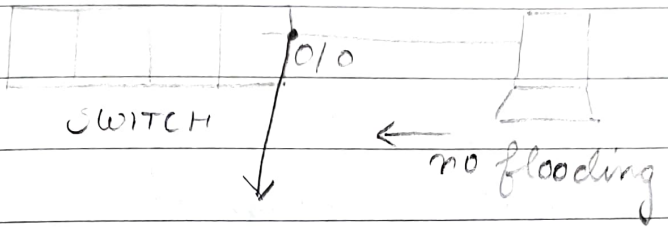
```
ip dhcp snooping
ip dhcp snooping VLAN 30
if# ip dhcp snooping trust
```

NOTE: no ip dhcp snooping info option 82

* ip dhcp snooping limit rate __
(limit DHCP message)

sw po-sec maximum -
" " mac-add 12a2.2acb.b215
" " " sticky

PORT SECURITY: prevents from mac-address flooding attack.



switchport port-security
sw po-sec violation restrict / shutdown / protect

DYNAMIC ARP INSPECTION (DAI): prevents from ARP poisoning.

whenever DAI used with DHCP snooping, it checks MAC-IP bindings & identify if MAC is correct or not.

ip arp inspection VLAN 10
if # ip arp inspection trust (each interface)

ip arp inspection validate src-mac
— — dst-mac
— — ip

CDP

DEFAULT TIME = 60 Second

HOLD TIME = 180 Second

CDP & LLDP :

- CDP is cisco proprietary & LLDP is IEEE.
- Both are used to verify neighbors in a network environment.

CDP TIMER : how often CDP packets are trans-mitted to all active interface

CDP HOLDTIME: delimits amount of time that device hold packets received from neighbors.

sh cdp → (Conf)# cdp run

cdp hold time → (Conf t)# cdp enable

cdp timer ↳ (interface)

sh cdp neighbor

— — — detail

LLDP: • Supported only on physical interfaces

- LLDP can discover one device per port.
- LLDP can discover LINUX servers.

	LLDP
lldp run	HOLDTIME = 120 Second
lldp transmit	DEFAULT TIME = 30 Second
lldp receive	

(Config #) enable secret / password
— username — password
service pass-encry

PASSWORDS & REMOTE ACCESS

Telnet: line vty 0 15
password ——
login
transport input telnet

SSH ip domain-name ——
crypto key generate rsa
—
ip ssh version —

(Config)#

line vty 0 15
login local
tran in ssh

— — —

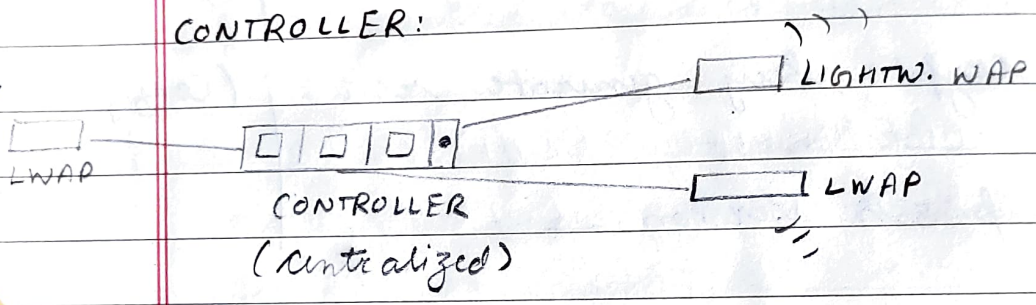
WIRELESS:

WAPs:

AUTONOMOUS WAP : • standalone
• with configuration interface

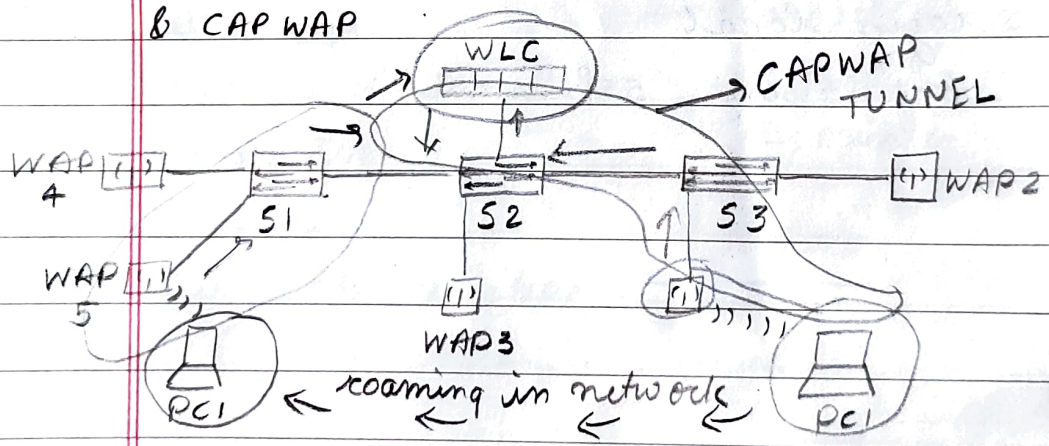
LIGHTWEIGHT WAP: • designed to be controlled by controller.

CONTROLLER:



SPLIT MAC:

& CAPWAP



- In split MAC design, if any device which is connected to a WAP, sends the data from WAP to S3 to WLC then to anybody.

- CAPWAP (Control & provisioning of WAP).

INTERFACE : → Management : management of IPs, etc.
LAG : combine all ports of WLC
→ WLC doesnt support LACP or PAGP
→ 8 connection max

* TACACS+ → 49 (TCP & UDP)
* RADIUS → 1812 (" ")

QoS

BRONZE → Bulk Data Transfer
SILVER → Basic user usage ex: transactional traffic
GOLD → lower priority sensitive protocol ex: intractive video
PLATINUM → time sensitive ex: VOIP phones.

- 802.11K → allow client devices to download neighboring WAP
- 802.11R → BSS fast transition (FT)
- 802.11E → QoS

VIRTUALIZATION

Vir. Components :

1. Hypervisor : It is 'the host' that runs a virtualization solution.

2. Vi. Guest : It is the virtual machine which runs on a host.

3. Vi. Appliance : It is a virtual solution provided by a vendor.
   - CISCO Service Router (CSR) 1000V
   - ASAV
   - Firepower

4. V-Switch : V-Switches allow hosts to assign VLANs to virtual machines.
   - STANDARD - DISTRIBUTED

5. Shared Storage : Accessing a SAN or NAS through iSCSI or Fibre Chan
   It permits all hosts in the network to access the same common storage.

6. Virtual Storage : With V. storage, each host utilize its local storage to create logical SAN across the net
   - CISCO Hyper Flex - VMWare Virtual SAN.

Virtualization Features:

1. Hardware Abstraction
2. Snapshots
3. Clones
4. Migrations

Virtualization Types:

1. TYPE 1: • Bare Metal Hypervisor.
   • entire server / OS is dedicated to virtualization.
   - VMWare ESXi
   - Hyper V
   - Xen

2. TYPE 2: • Desktop Virtualization
   - VMWare Workstation / Fusion
   - Virtualbox
   - KVM

AUTOMATION:

JSON:
- Javascript Object Notion.
- Structured & human readable.
- Uses double quotes

Ex:

```
{
  "People" : [
    {
      "name" : "ABC",
      "Age" : "20",
      "Address" : "1NZ, 52, TX, US"
    },
    {
      "name" : "DEF",
      "Age" : "24",
      "Address" : "25 DS, DA, AZ, US"
    }
  ]
}
```

REST API: APIs allow you to quickly access an application resource without manually mapping out the applicatio

REST

Representational State Transfer

CRUD

C	CREATE	Post
R	READ	Get
U	UPDATE	Put / Patch
D	DELETE	Delete

200	OK
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not found
500	Internal Server Error
503	Service Unavailable

PLANES:

① Management:

- controls everything about logging in to a network
- Telnet & SSH Access.
- HTTP & HTTPS

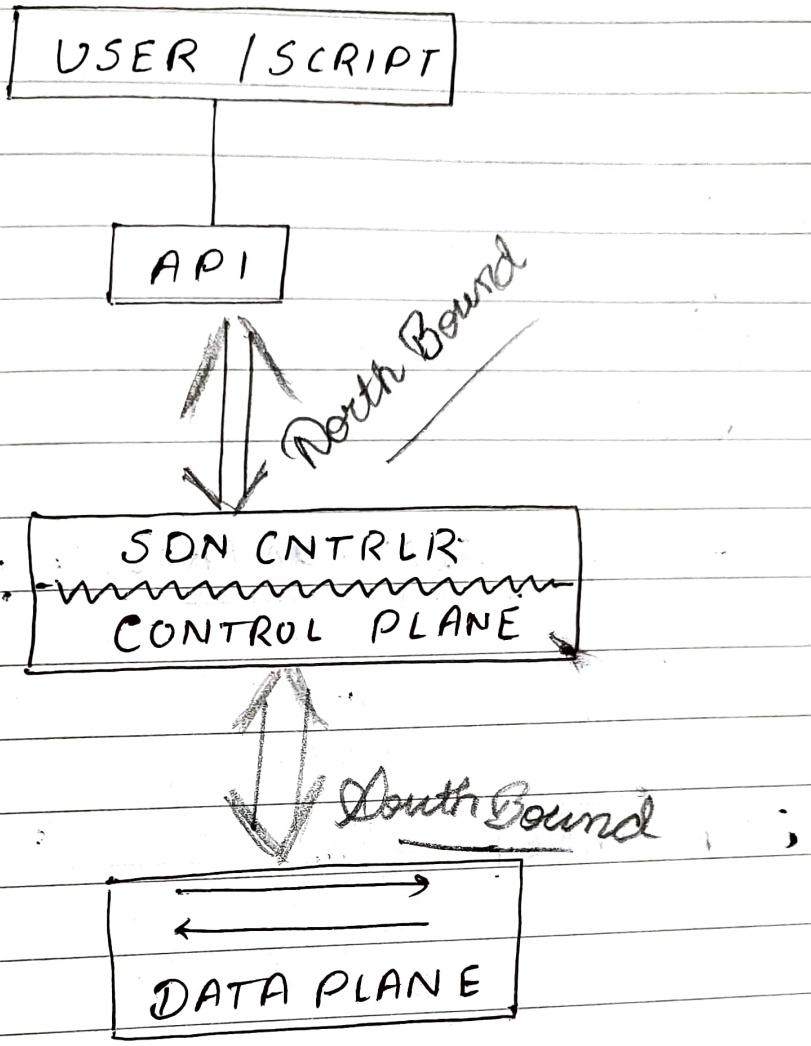
② Control:

- Brain of the router / switch
- ACL, NAT, OSPF
- STP, VTP, MAC
- QoS, CDP, LLDP

③ Data:

- workhouse of R/S.
- this plane directly affects traffic.
- encapsulation / Decapsulation.
- dropping traffic.

NORTH BOUND / SOUTHBOUND



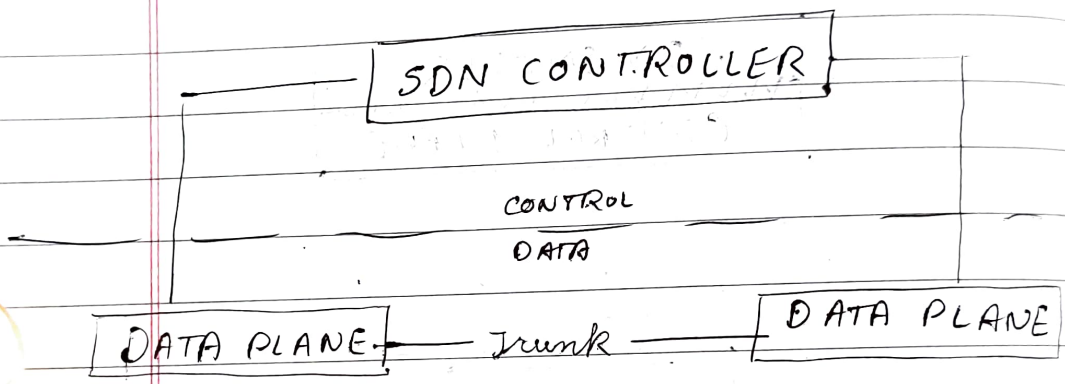
NB: We access SDN controller through North Bound Interface.

→ We can done work in controller via
- MERAKI (GUI)
- Restful API inside a script.

- creating VLAN.
- getting list of N/W devices.
- polling health of N/W devices.

SB: SBI, how SDN controller talks to actual devices.
there are lots of different ways:

- Open Flow
- Netconf
- opflex
- OnePK



Underlay → Physical network that provides connectivity.
MTU, Interface, OSPF | ISIS, Verification

Overlay → Virtual Network tunneled over underlay.
→ Virtual Extensible LAN (VXLAN) is a way to do it.

Fabric → All L3 devices.
Simple high speed L3 network

Date
Page

☆ CISCO DNA CENTER FEATURES:

Discovery: CDP / LLDP, automatically discovers devices.

Hierarchy: Allows us to organize our networks into sites & locations.
→ can fully manage wireless environment.

Templates: Specific configuration pushing.

Upgrades: makes firmware updates easier.
→ bunch of automatic check before upgrade.

Command Runner: can access many devices at once.
→ lets us to run a bunch of commands against device & store the results.

Assurance: → time machine.
→ saves everything for a week.
→ correlates issues & suggestion provider.

Path Trace: DNA center knows everything about all network devices.
→ visual representation of packet travel from source to dest.

→ Easy QoS : → Buisniss Relvant.
→ Buisniss Irrelvant.
→ Default.

→ LAN Automation → PNP (plug & play)

→ SD Accss. → Intent Based Networking

→ Restful API : DNA centre can be managed by REST.

CAMPUS — CORE
— DISTRIBUTION
— ACCESS

CLOS - SPINE
- LEAF