SHREE COMP SYSTEMS NAGPUR

PROJECT DOCUMENTATION

Up-gradation/Expansion of Data Center and Campus Wide Network at Government College of Engineering Kathora Naka Amravati

The project documentation is in accordance to:
Tender notice no. GCOEA/CWN-DC/2020/553 dated: 31/01/2020 and
Corrigendum GCOEA/CWN-DC/2020/553/31/1/20 dated 11/02/2020
Purchase Order NO.GCOEAlCWN-DC/2020/1416 dated 27.03.2020
Agreement for Upgradation/Expansion of Datacenter and campus wide network dated 24.08.2020 signed by Shree Comp Systems Nagpur The Principal. CWN Committee Members of GCOE Amravati on dated 24.08.2020

Dated: 10th August 10, 2021 **Place: Nagpur**

ACKNOWLEDGEMENT

We have pleasure in submitting you this valuable ***PROJECT REPORT*** as a useful document containing design details & as built layout with request to preserve the same till the life of equipment, as can be referred in future while carrying out modification & trouble shooting.

We once again take this as an opportunity to convey thanks for awarding us the prestigious chance of providing our services to you.

Special thanks to:

- Dr. R.P.Borkar Sir Honorable Principal GCOE Amravati
- Dr. Premchand Ambhore Sir CWN Project In-Charge
- Shri. Gunwant Dhomne Sir CWN Project Committee Chairman
- Shri. Dilip Uike Sir CWN Project Committee Member
- All Respected Committee Members, Faculties and Staff

Table of content:

SHREE COMP SYSTEMS

9 Corporation Colony, Prashant Nagar, Besides FCI Godown, Ajni, Nagpur 440015
Tel No.: 0712-2250127 Cell No 9373109434 / 9112390753 www.shreecompsystems.com

The Principal
Government College of Engineering
Amravati 444604

Date: 23.12.2020
Ref: SCS/20-21/CL1

REF: Purchase Order NO.GCOEAlCWN-DC/2020/1416 dated 27.03.2020 for Upgradation / Extension of Data Centre and Campus Wide Network and subsequent extension for project completion till 27.12.2020.

SUB: Regarding Project Installation and configuration Completion Report.

Dear Sir,

With reference to above mentioned subject please note that the installation, configuration and testing of all devices as per Annexure A, B, C, D, E of above referred PO was duly completed.

On 23.12.2020, we have provided the details of configuration and done physical verification of installed material in datacenter and all user departments along with committee members of institute.

We request you to please sign this report as a token of acceptance.

Thanking you and assuring you of our best service at all times.

Yours faithfully
Shree Comp Systems
Nagpur

Atul Patil
9112390753

Project Overview

Project Challenge Summary

- Deliver an expanding roster of network-based educational applications to a growing community of users using a wide range of devices.
- Ensure the reliability, availability and security of a campus-wide combined wired and wireless network.
- Providing latest 10G fiber backbone to individual departments in campus.
- Providing latest Wifi6 wireless network connectivity to all users-students, staff and faculty in the campus.

Network Implementation Summary

- Cisco 4-slot chassis switches in HA, distribution and access layer spread across department in Campus.
- Wireless Lan Controller with latest Wifi6 indoor and outdoor wireless access points.
- Network management at-a-glance using Cisco Prime Infrastructure NMS.
- Windows 2012 Server ADDS DNS and NTP implementation.
- Cisco router bundled with Communication Management Express license for seamless telephony among user in departments of campus.

Business Result Summary

- Robust network availability and reliability with almost 99% uptime (report enclosed).
- Enhanced network security and manageability.
- Improved and consistent network availability required to provide high quality education.

Product List

Switching

- Cisco C9404R Cisco Catalyst 9400 Series 4 slot chassis
- Cisco C9200L-24P-4G-E Catalyst 9200L 24-port PoE+, 4 x 1G
- Cisco C9200L-24P-4X-E Catalyst 9200L 24-port PoE+, 4 x 10G

Firewall

- Cisco FPR2110-NGFW-K9 Cisco Firepower 2110 NGFW Appliance

Controllers

- Cisco AIR-CT3504-K9 Cisco 3504 Wireless Controller

Access Points:

- Cisco C9120AXI-D Cisco Catalyst 9120AX Series
- AIR-AP1562E-D-K9 802.11ac W2 Low-Profile Outdoor AP, External Ant

Router:

- ISR4321-V/K9 Cisco ISR 4321 Bundle
- L-CME-CUE Communication Manager Express (CME)

IP Phones:

- CP-3905= Cisco Unified SIP Phone 3905
- CP-7821-K9= Cisco UC Phone

Video Conferencing

- CS-KITPLUS-K9 Room Kit Plus Codec Plus, Quad Camera and Touch 10

Network Management:

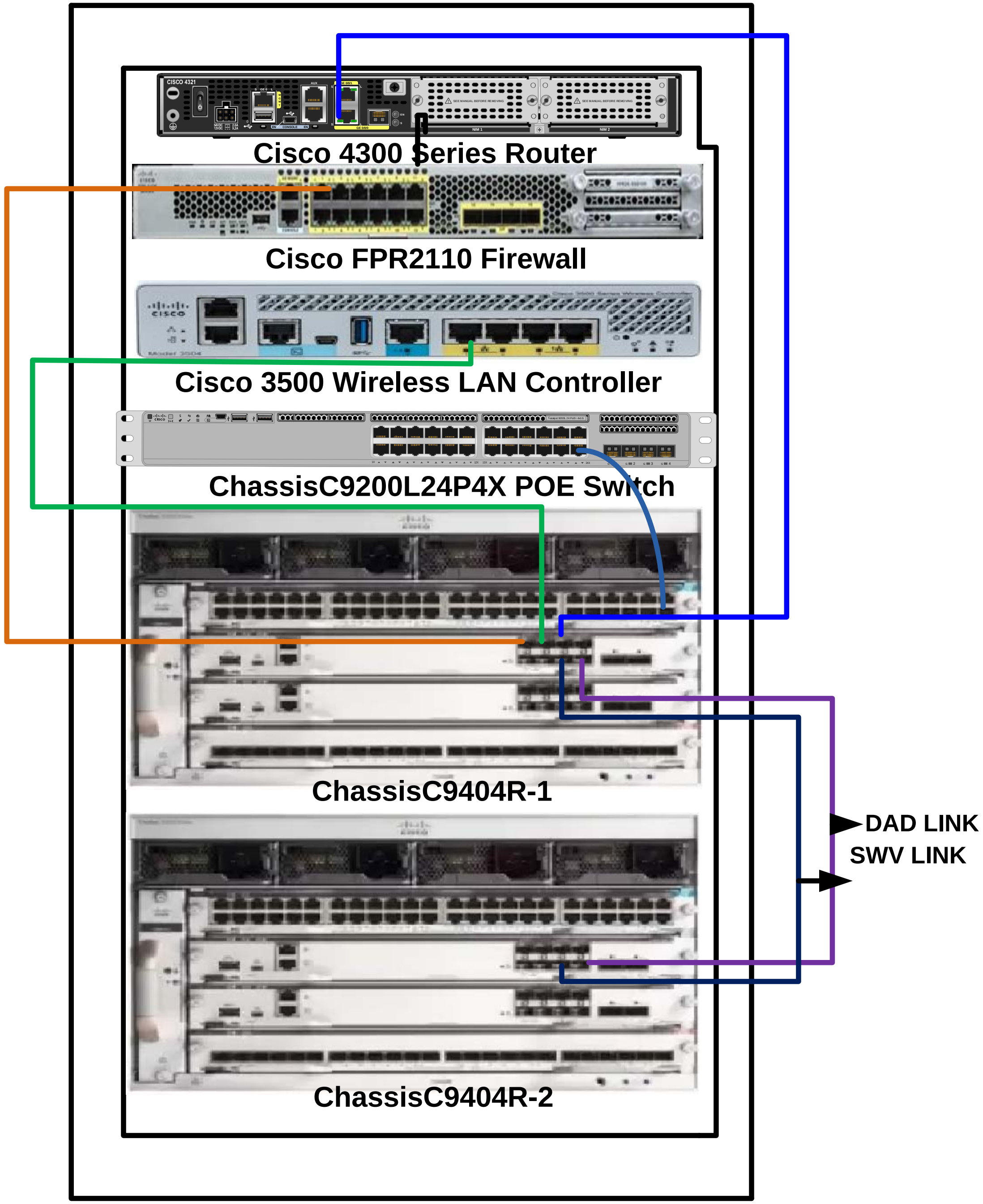
- R-MGMT3X-N-K9 Cisco Ent MGMT: Lic For Prime Infrastructure 3.x

NETWORK DIAGRAMS:

Please find enclosed network diagrams as below:

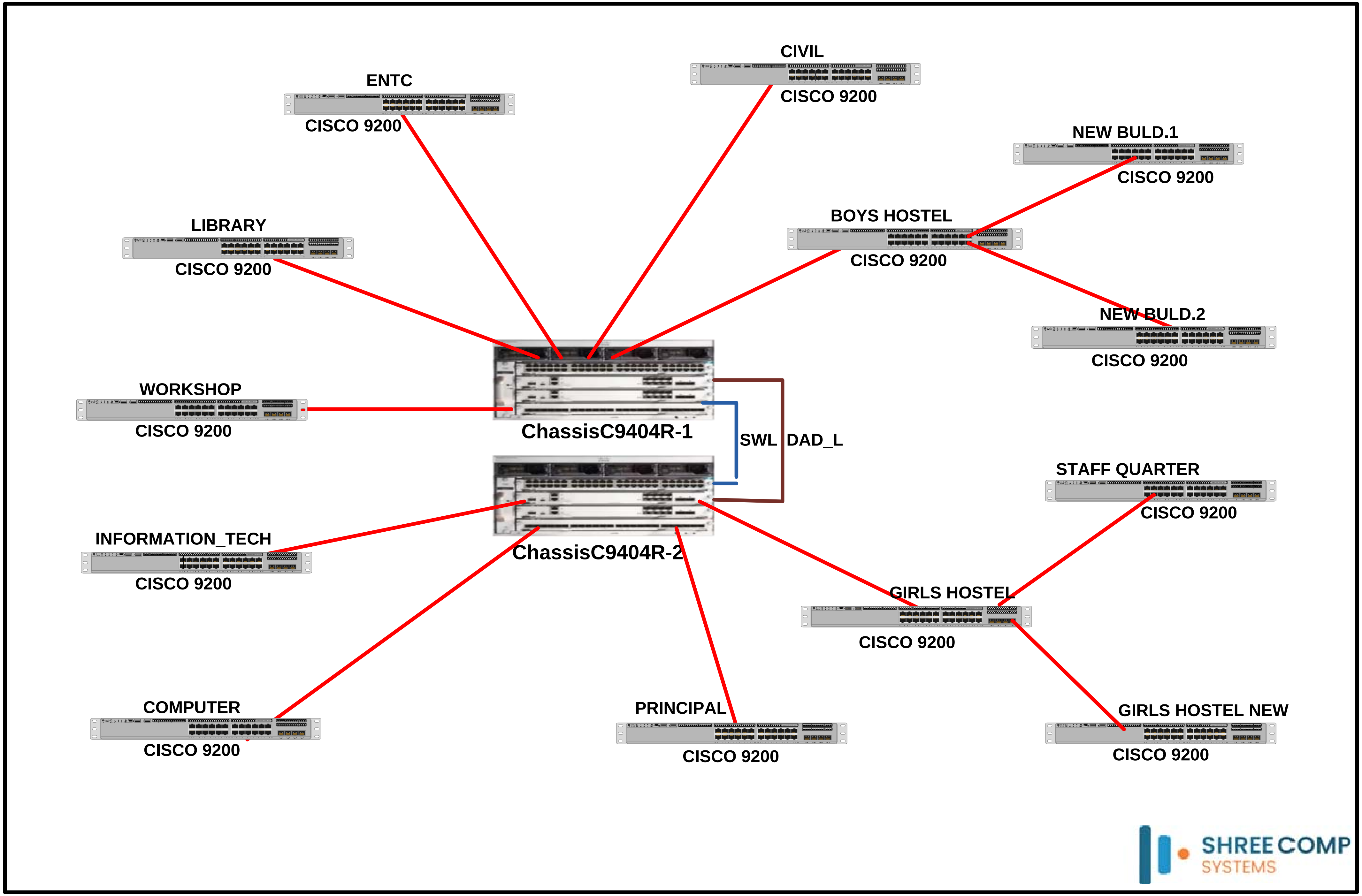
- Fiber network layout map
- CWN network devices map
- Civil department existing and new network devices connectivity map
- Girls hostel new network devices connectivity map
- Girtls hostel_1 network devices connectivity map
- Computer department existing and new network devices connectivity map
- ENTC department existing and new network devices connectivity map
- IT department existing and new network devices connectivity map
- Library new network devices connectivity map
- Principal quarter new network devices connectivity map

GCOEA DATACENTER NETWORK RACK

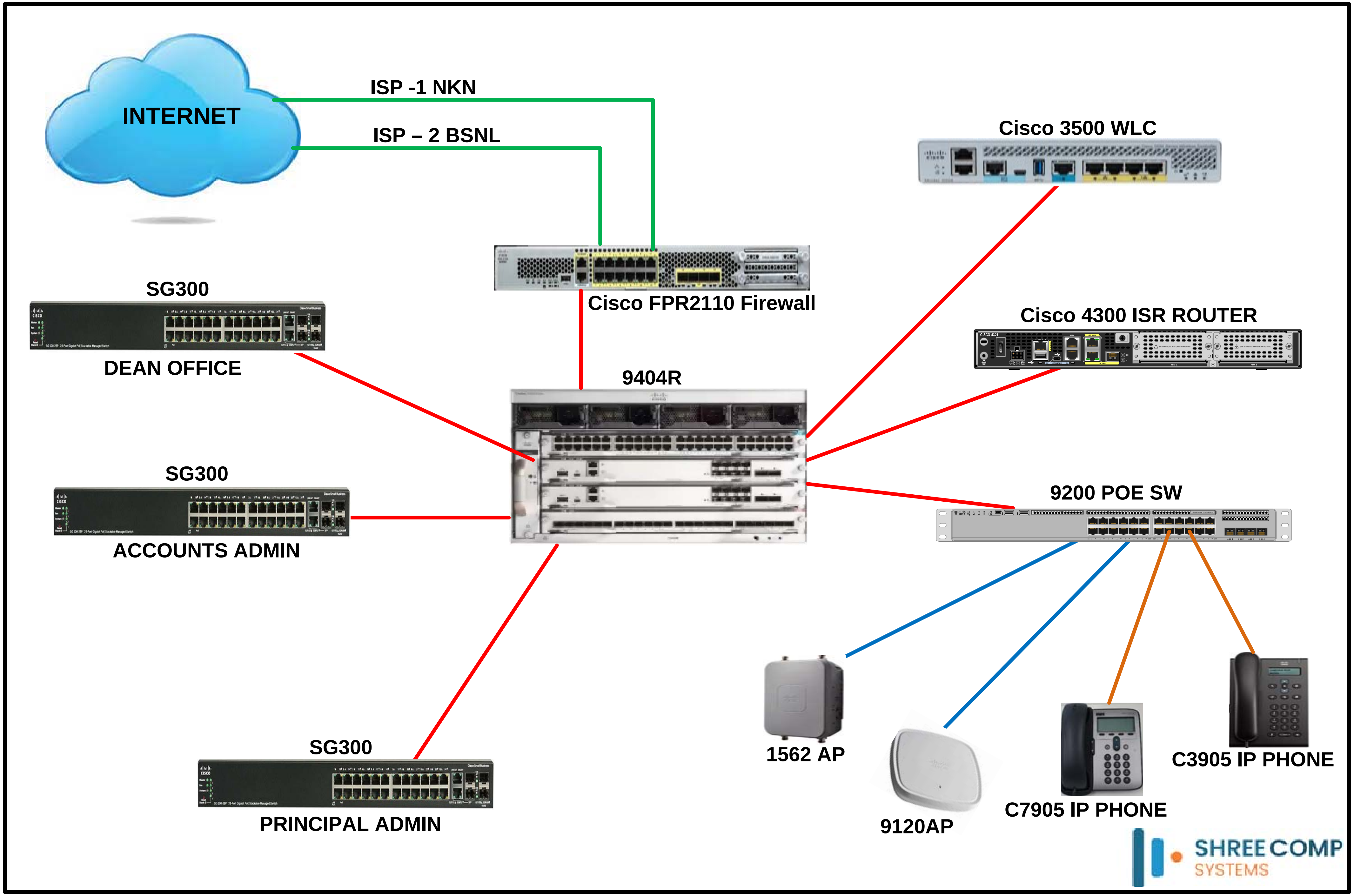


SHREE COMP SYSTEMS

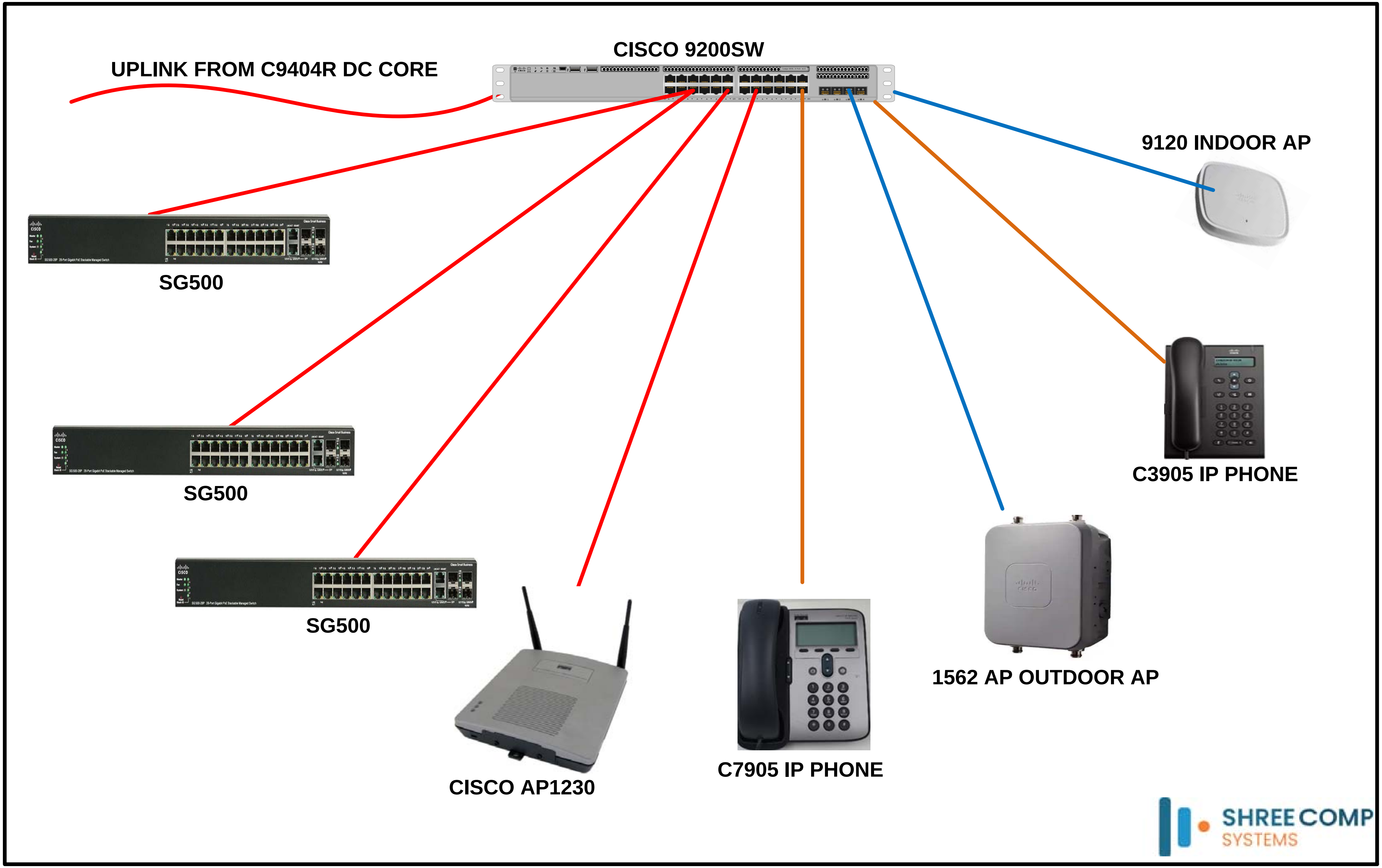
FIBER NETWORK LAYOUT MAP



CWN NETWORK DEVICES MAP

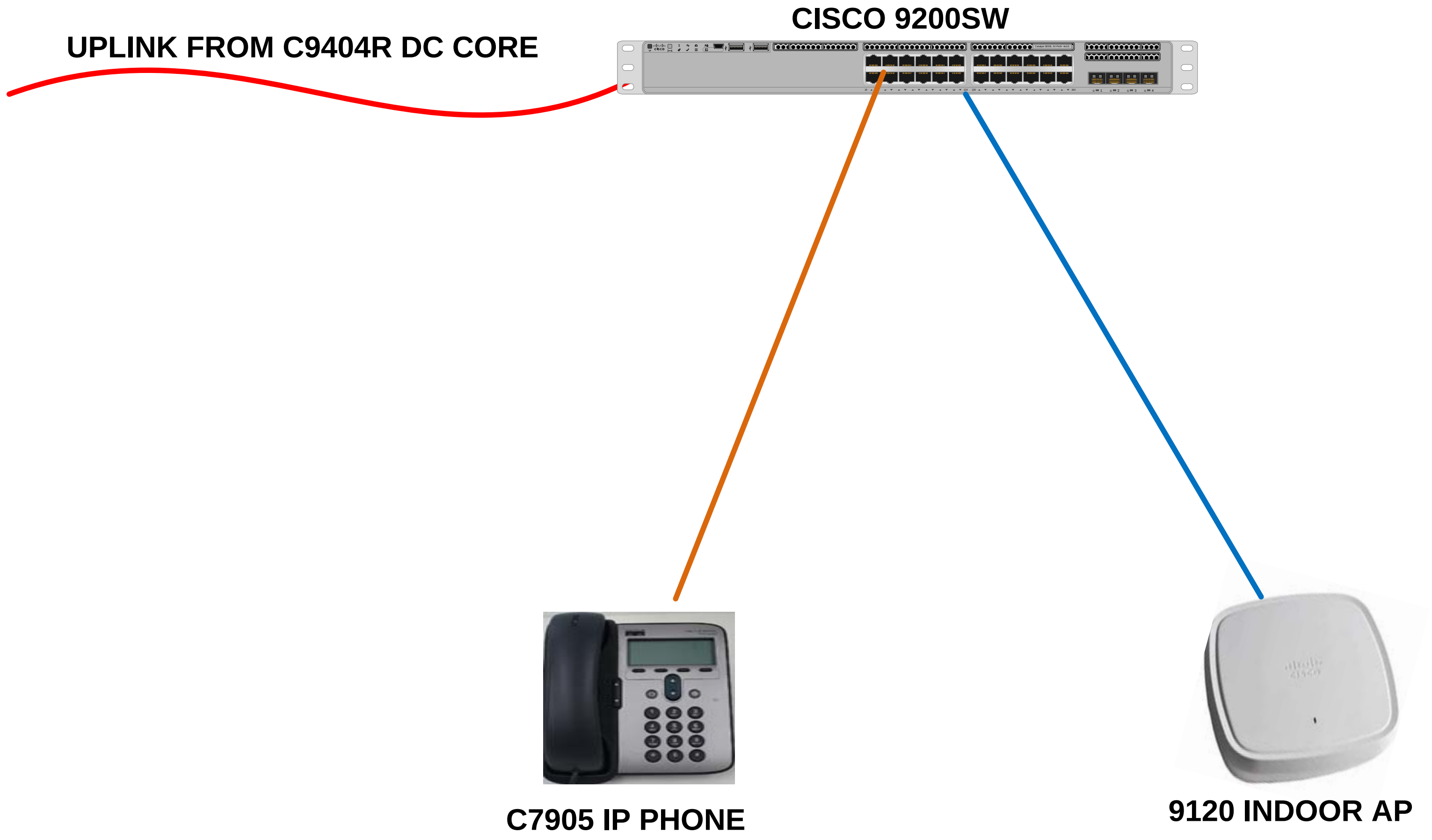


CIVIL DEPT. EXITING & NEW NETWORK DEVICES CONNECTIVITY MAP



SHREE COMP SYSTEMS

GIRLS HOSTEL NEW NETWORK DEVICES CONNECTIVITY MAP



CISCO 9200SW

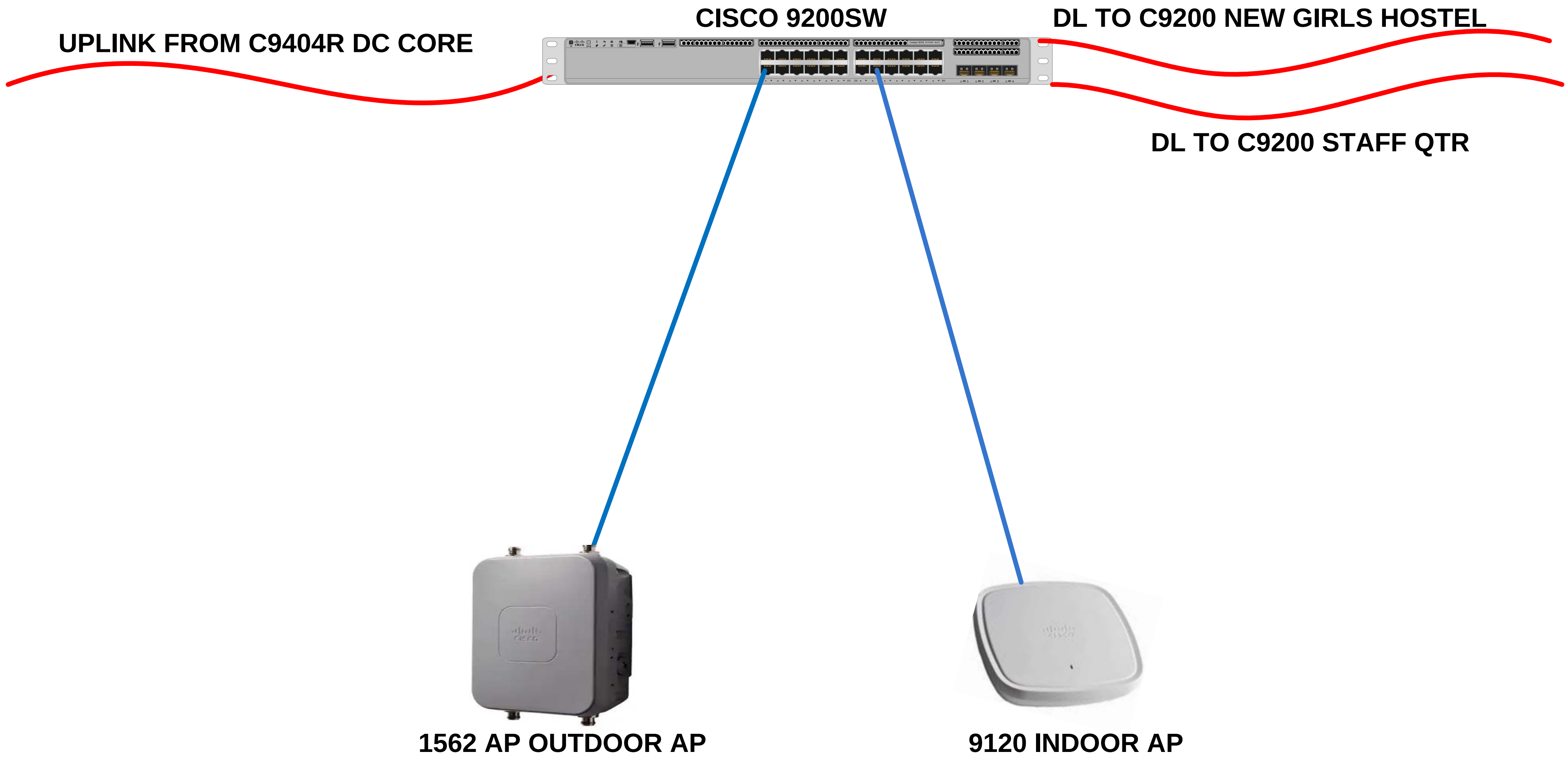
UPLINK FROM C9404R DC CORE

C7905 IP PHONE

9120 INDOOR AP

SHREE COMP
SYSTEMS

GIRLS HOSTEL_1 NETWORK DEVICES CONNECTIVITY MAP



CISCO 9200SW

UPLINK FROM C9404R DC CORE

DL TO C9200 NEW GIRLS HOSTEL

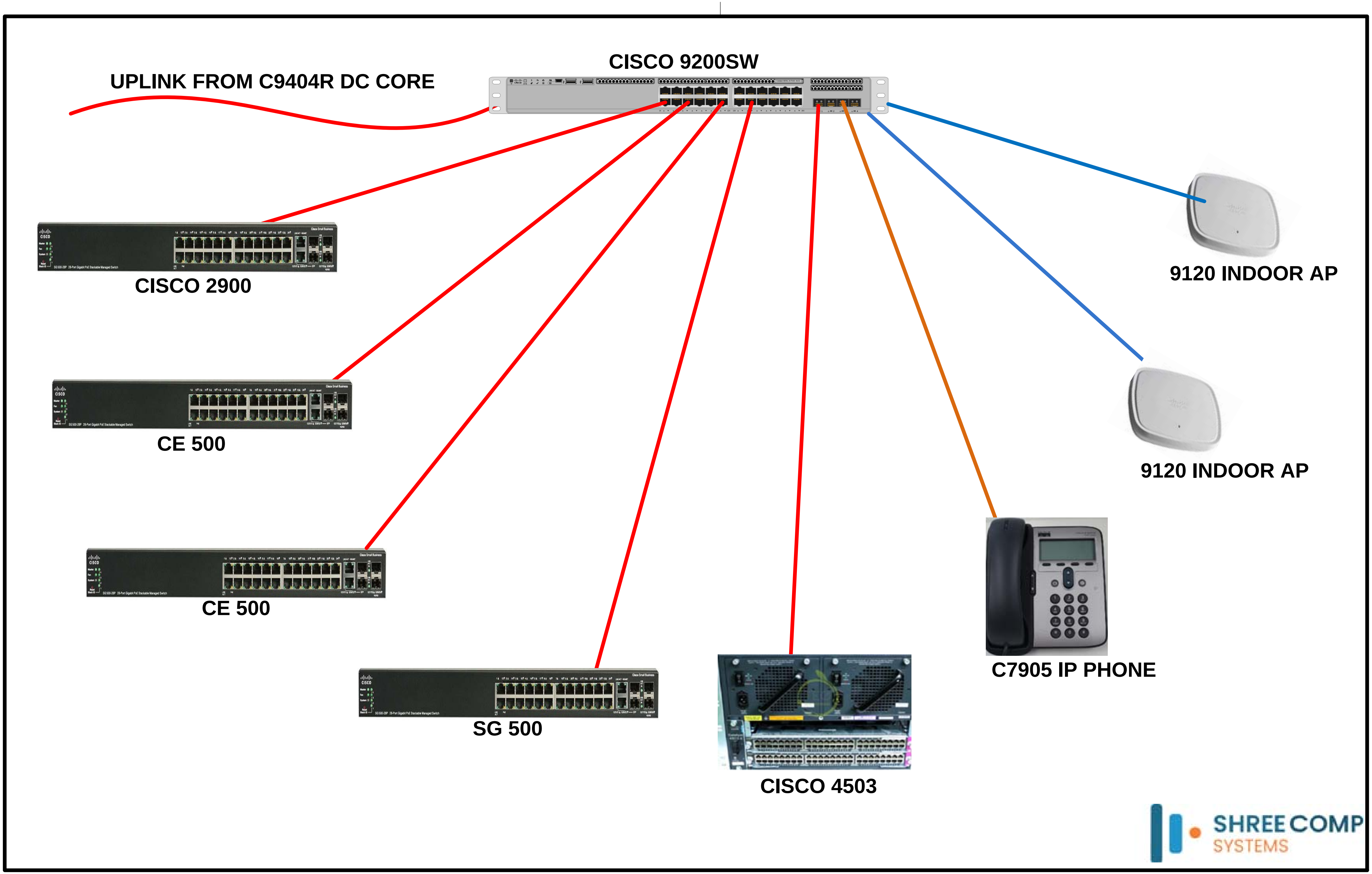
DL TO C9200 STAFF QTR

1562 AP OUTDOOR AP

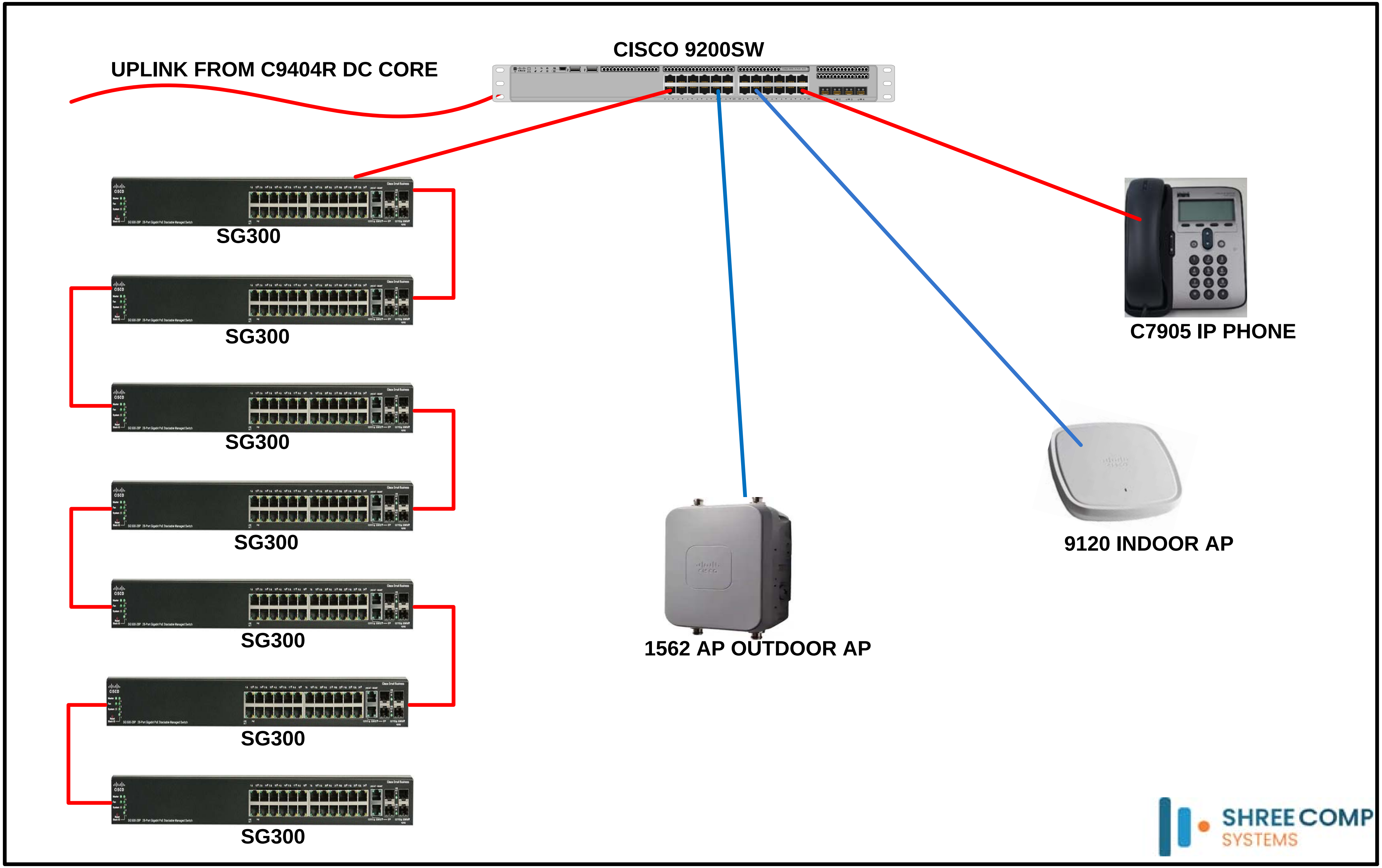
9120 INDOOR AP

SHREECOMP
SYSTEMS

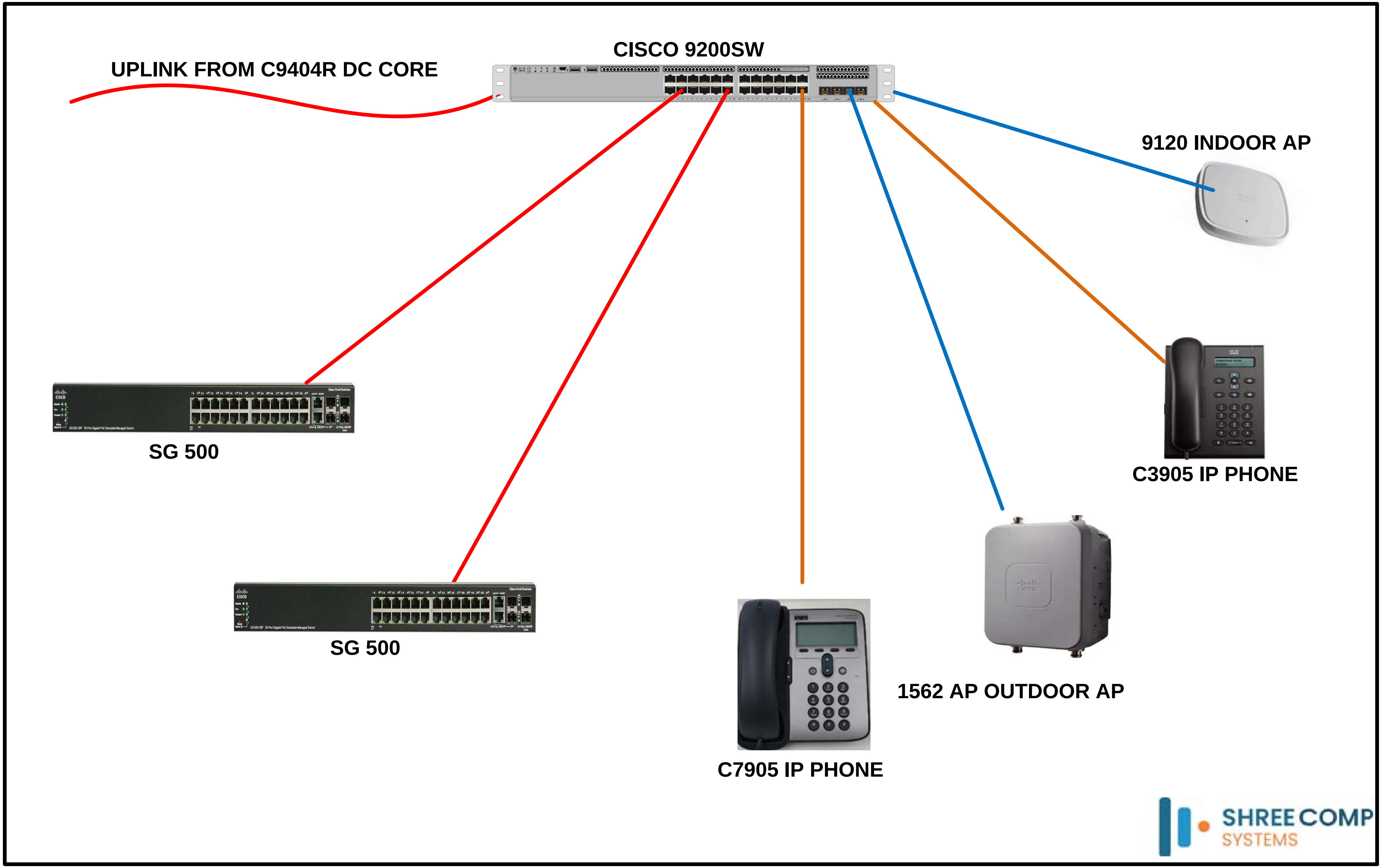
COMPUTER DEPT. EXITING & NEW NETWORK DEVICES CONNECTIVITY MAP



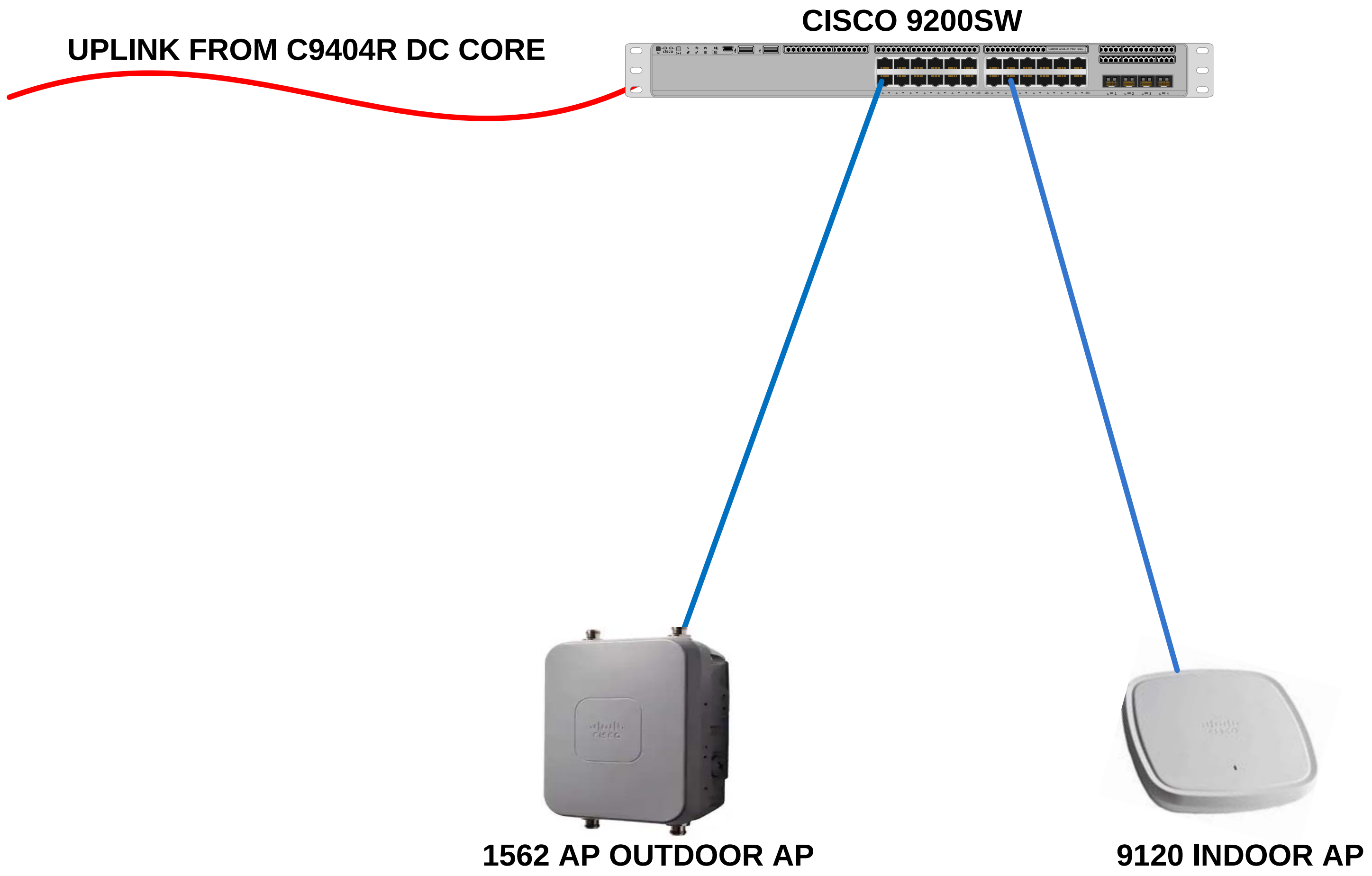
ENTC NETWORK DEVICES CONNECTIVITY MAP



IT DEPT. EXITING & NEW NETWORK DEVICES CONNECTIVITY MAP

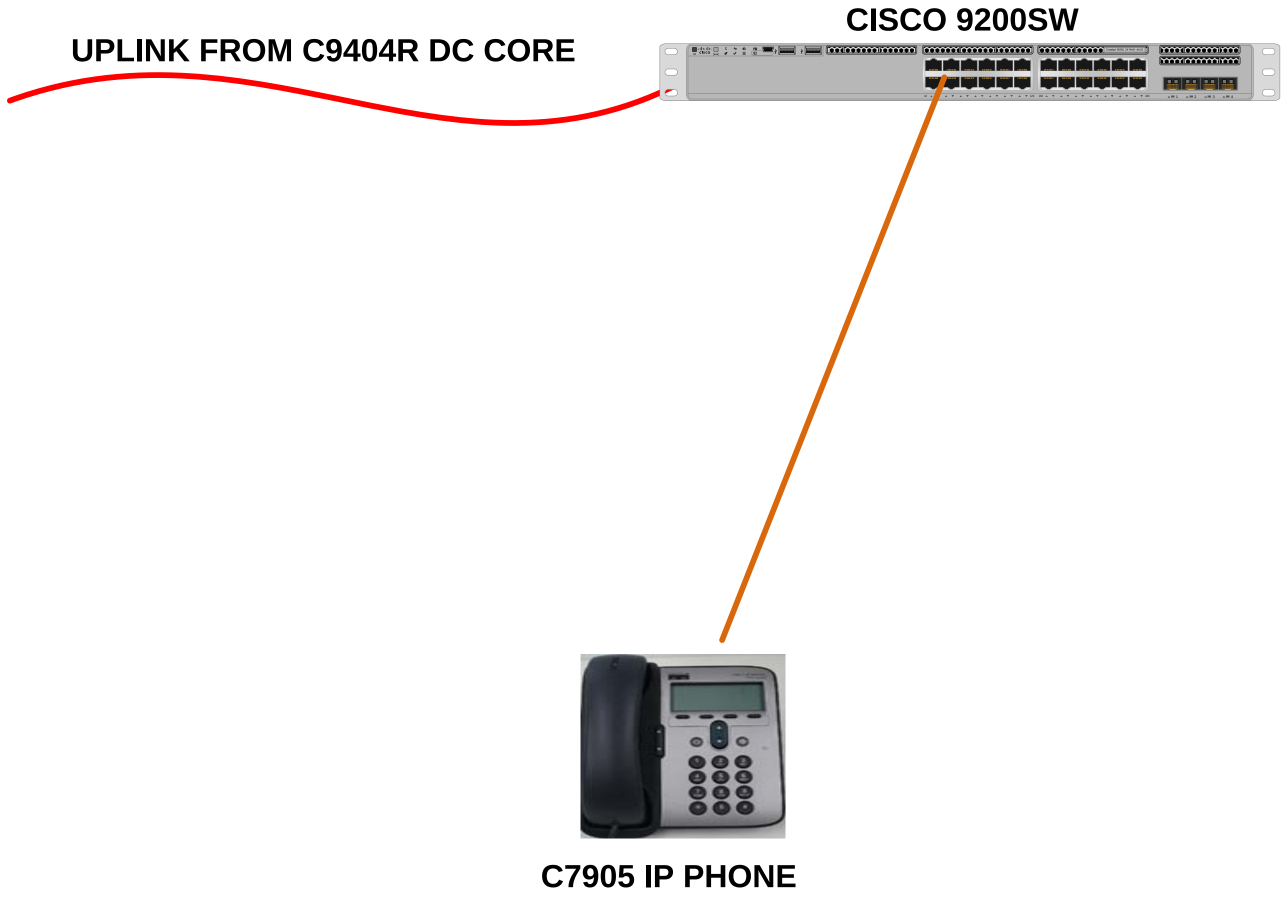


LIBRARY NETWORK DEVICES CONNECTIVITY MAP

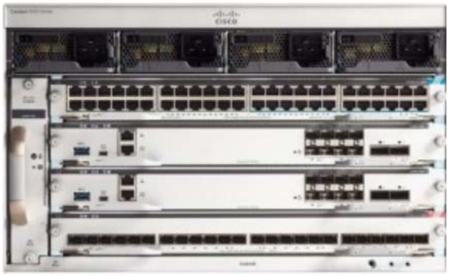


SHREE COMP SYSTEMS

PRINCIPAL QTR NETWORK DEVICES CONNECTIVITY MAP



SHREE COMP
SYSTEMS



Cisco C9404R Cisco Catalyst 9400 Series 4 Slot Chassis

The Cisco Catalyst® 9400 Series switches are Cisco's leading modular enterprise switching access, distribution and core platform built for security, IoT and cloud. These switches form the foundational building block for SD-Access — Cisco's lead enterprise architecture. The platform provides unparalleled investment protection with a chassis architecture that is capable of supporting up to 9 Tbps of system bandwidth and unmatched power delivery with high density IEEE 802.3bt PoE (60W and 90W). Redundancy is now table stakes across the portfolio.

The Catalyst 9400 delivers state-of-the-art High Availability (HA) with capabilities like Cisco StackWise® Virtual technology with In-service-software-upgrade (ISSU), SSO/NSF, uplink resiliency, N+1/N+N redundancy for power supplies. The platform is enterprise optimized with an innovative dual-serviceable fan tray design, side to side airflow and is closet-friendly with ~16" depth. A single system can scale up to 384 access ports with your choice of 5G multigigabit copper, 1G copper, 1G fiber, Cisco UPOE®+, Cisco UPOE and PoE+ options and up to 192 ports of 10G Fiber and 10G multigigabit options.

The availability of 1/10 G fiber ports facilitate aggregation of existing small form factor fixed access switches. The addition of the new SUP-1XL-Y supervisor allows unique investment protection through 25 G uplink connectivity option which is becoming a popular alternative to 10 G in the core.

The platform also supports advanced routing and infrastructure services, SD-Access capabilities and network system virtualization. These features enable optional placement of the platform in the core and aggregation layers of small to medium-sized campus environments.

The Catalyst 9400 Series chassis is enterprise optimized with efficient side-to-side airflow and full front accessibility for all removable components, including supervisors, line cards, power supplies and fan tray. The chassis also supports optional rear accessibility for fan trays to enable efficient cable management. Catalyst 9400 Series chassis, supervisor, line cards, powersupply and fan trays have embedded RFID tags which facilitate easy asset and inventory management using commercial RFID readers.

Cisco C9404R Deployment Includes:

- Configuring management interface
- Configuring stackwise virtual links (SVL) to stack two switches
- Configuring dual-active-detection links (DAD) to deploy the switch stack in active-active state
- Configuring the ip domain name, ip name-servers and NTP server
- Registration of switch for DNA licensing using Cisco Smart Licensing Portal
- Formation of Vlans
- Configuring VTP and setting switch VTP mode as server
- Configuring Vlan interfaces
- Assigning ports to Vlans
- Configuring DHCP server for created Vlans, exclusion of IP address for static use
- Configuring layer3 route
- Configuring auto backup of switch stack running configuration for disaster recovery
- Enabling switch stack GUI access
- Assigning banner to switch stack

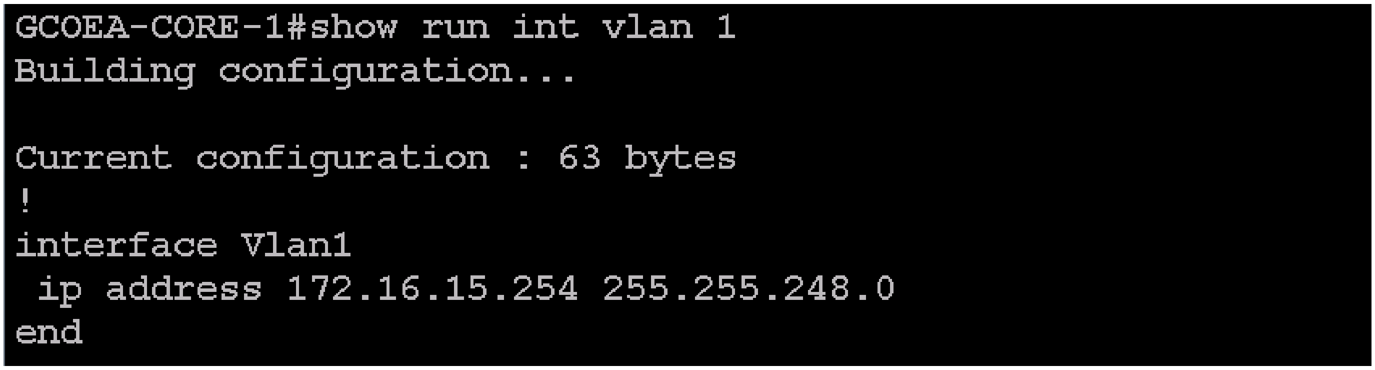
The C9404R is a 4 slot chassis switch populated with C9400-LC-48T= 48-Port 10/100/1000 (RJ-45) line card and C9400-SUP-1XL Cisco Catalyst 9400 Series Supervisor 1XL Module 3nos. The active switch is populated with 2nos of C9400-SUP-1XL Cisco Catalyst 9400 Series Supervisor 1XL Module and C9400-LC-48T= 48-Port 10/100/1000 (RJ-45) and the standby switch is populated with 1nos of C9400-SUP-1XL Cisco Catalyst 9400 Series Supervisor 1XL Module.

The C9400-SUP-1XL Cisco Catalyst 9400 Series Supervisor 1XL Module is having 8x10G SFP+ slots and 2 Uplink slots. We have terminated the departmental backbone fiber links of the SUP SFP+ slots. Refer supervisor image as below:

Configuring management interface:

To manage the Cisco switch, we need to configure a management interface. Unlike the routers that allow for management on any configured interface.

The configured management interface of C9404R is as below:

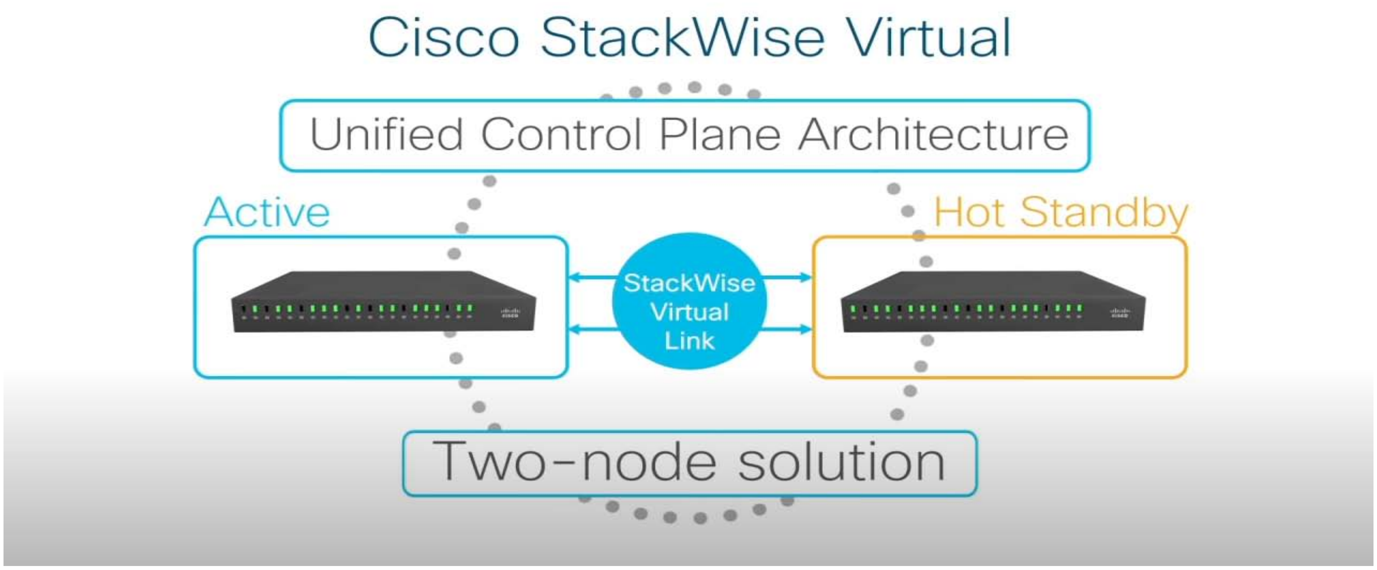


```
GCOEA-CORE-1#show run int vlan 1
Building configuration...

Current configuration : 63 bytes
!
interface Vlan1
 ip address 172.16.15.254 255.255.248.0
end
```

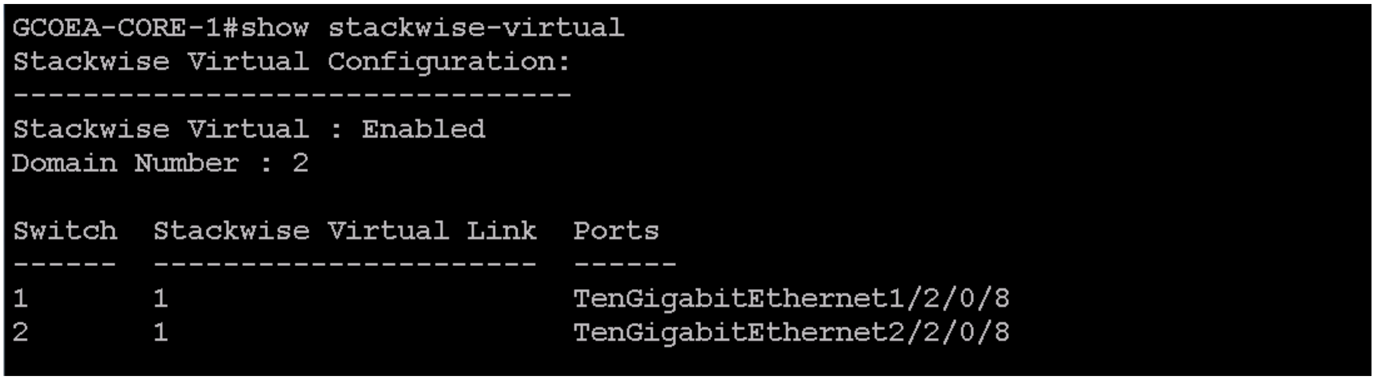
Configuring stackwise virtual link (SVL):

StackWise Virtual Overview

Cisco StackWise Virtual is a network system virtualization technology that pairs two switches into one virtual switch. Switches in a Cisco StackWise Virtual solution increase operational efficiency by using single control and management plane, scale system bandwidth with distributed forwarding plane, and assist in building resilient networks using the recommended network design. Cisco StackWise Virtual allows two physical switches to operate as a single logical virtual switch using a 40G or 10G Ethernet connection. Deployment example is as below:

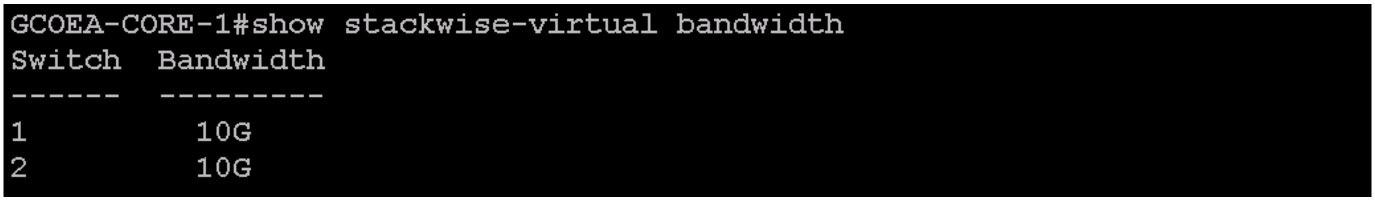


The configured stackwise virtual link is as below:



```
GCOEA-CORE-1#show stackwise-virtual
Stackwise Virtual Configuration:
--------------------------------
Stackwise Virtual : Enabled
Domain Number : 2

Switch  Stackwise Virtual Link  Ports
------  ----------------------  ------
1       1                       TenGigabitEthernet1/2/0/8
2       1                       TenGigabitEthernet2/2/0/8
```

The stackwise virtual link is configured using 10G interface on Supervisor. Refer image as below for bandwidth summary:



```
GCOEA-CORE-1#show stackwise-virtual bandwidth
Switch  Bandwidth
------  ---------
1         10G
2         10G
```

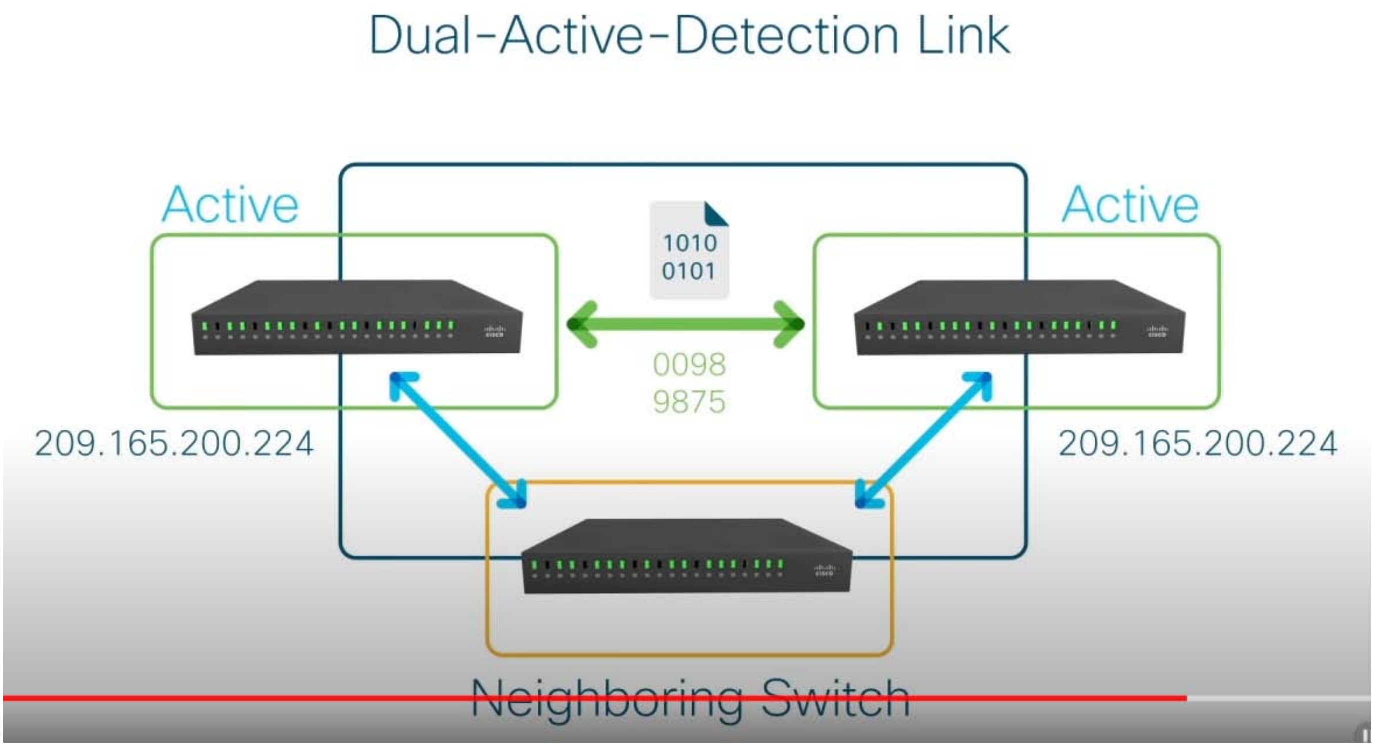
Configuring dual-active-detection link (DAD):

Dual-Active Detection

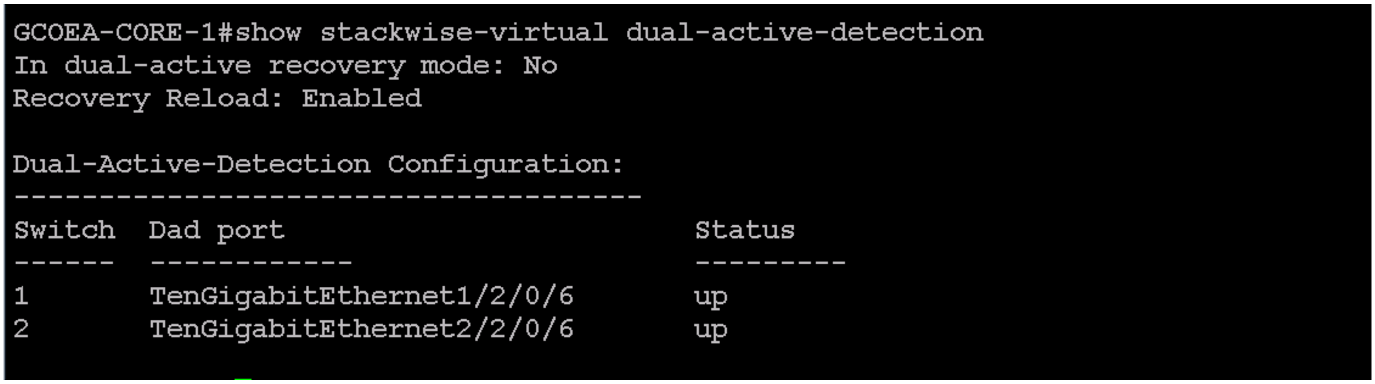
If the original Cisco StackWise Virtual active switch is still operational, both the switches will now be Cisco StackWise Virtual active switches. This situation is called a dual-active scenario. This scenario can have adverse effects on network stability because both the switches use the same IP addresses, SSH keys, and STP bridge IDs. Cisco StackWise Virtual detects a dual-active scenario and takes recovery action. Dual-active-detection link is the dedicated link used to mitigate this.

If a StackWise Virtual link fails, the Cisco StackWise Virtual standby switch cannot determine the state of the Cisco StackWise Virtual active switch. To ensure that switchover occurs without delay, the Cisco StackWise Virtual standby switch assumes that the Cisco StackWise Virtual active switch has failed and initiates switchover to take over the Cisco StackWise Virtual active role.

The deployment concept of DAD is as below:

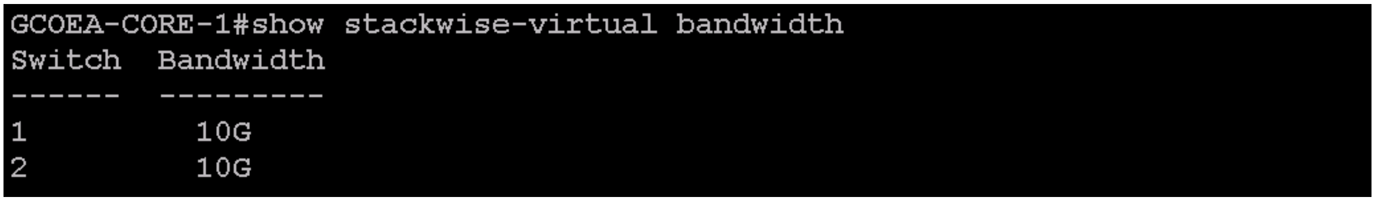


The configured stackwise virtual dual active detection link is as below:



```
GCOEA-CORE-1#show stackwise-virtual dual-active-detection
In dual-active recovery mode: No
Recovery Reload: Enabled

Dual-Active-Detection Configuration:
-------------------------------------
Switch  Dad port                        Status
------  ------------                    ---------
1       TenGigabitEthernet1/2/0/6       up
2       TenGigabitEthernet2/2/0/6       up
```

The stackwise virtual link is configured using 10G interface on Supervisor. Refer image as below for bandwidth summary:



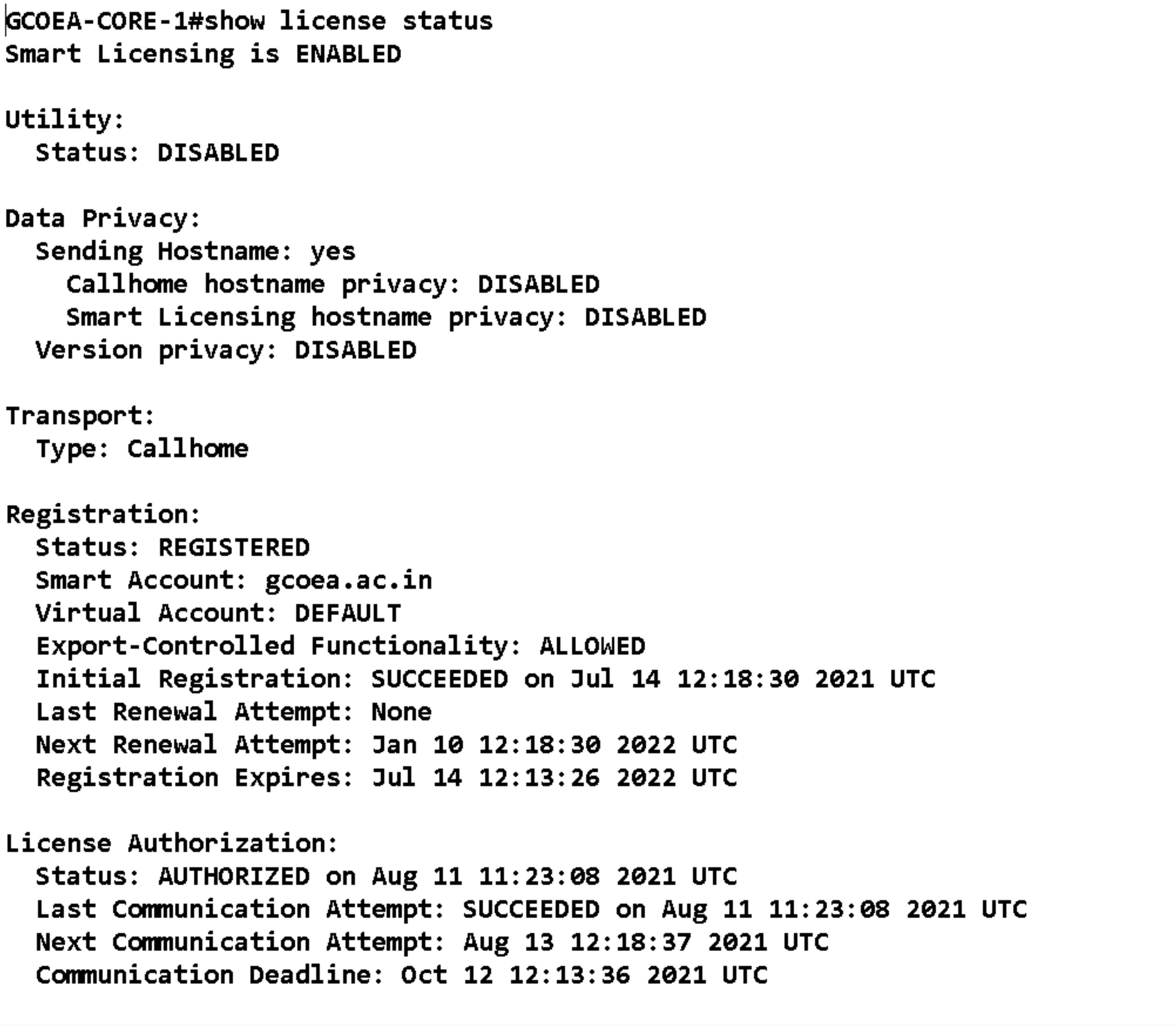
```
GCOEA-CORE-1#show stackwise-virtual bandwidth
Switch  Bandwidth
------  ---------
1         10G
2         10G
```

Registration of switch stack for DNA licensing using Cisco Smart Software Licensing Portal:

Information about Smart Licensing

Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends. Smart Licensing helps simplify three core functions:

- Purchasing
- Management
- Reporting



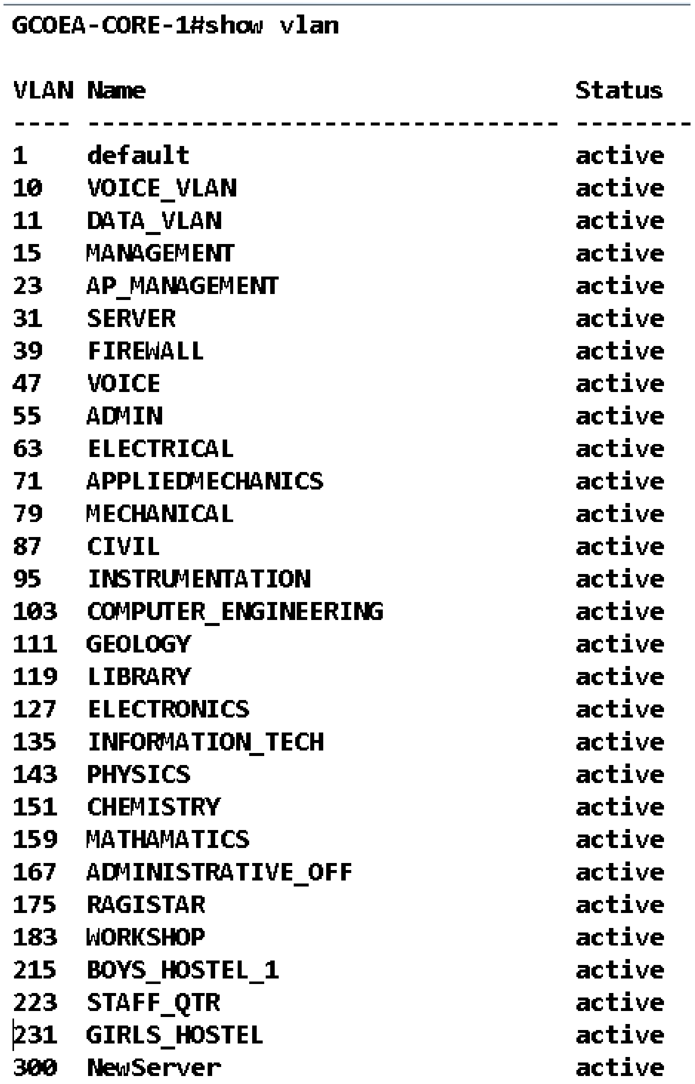
```
GCOEA-CORE-1#show license status
Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: gcoea.ac.in
  Virtual Account: DEFAULT
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Jul 14 12:18:30 2021 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 10 12:18:30 2022 UTC
  Registration Expires: Jul 14 12:13:26 2022 UTC

License Authorization:
  Status: AUTHORIZED on Aug 11 11:23:08 2021 UTC
  Last Communication Attempt: SUCCEEDED on Aug 11 11:23:08 2021 UTC
  Next Communication Attempt: Aug 13 12:18:37 2021 UTC
  Communication Deadline: Oct 12 12:13:36 2021 UTC
```

Formation of Vlans:

Overview of VLANs

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

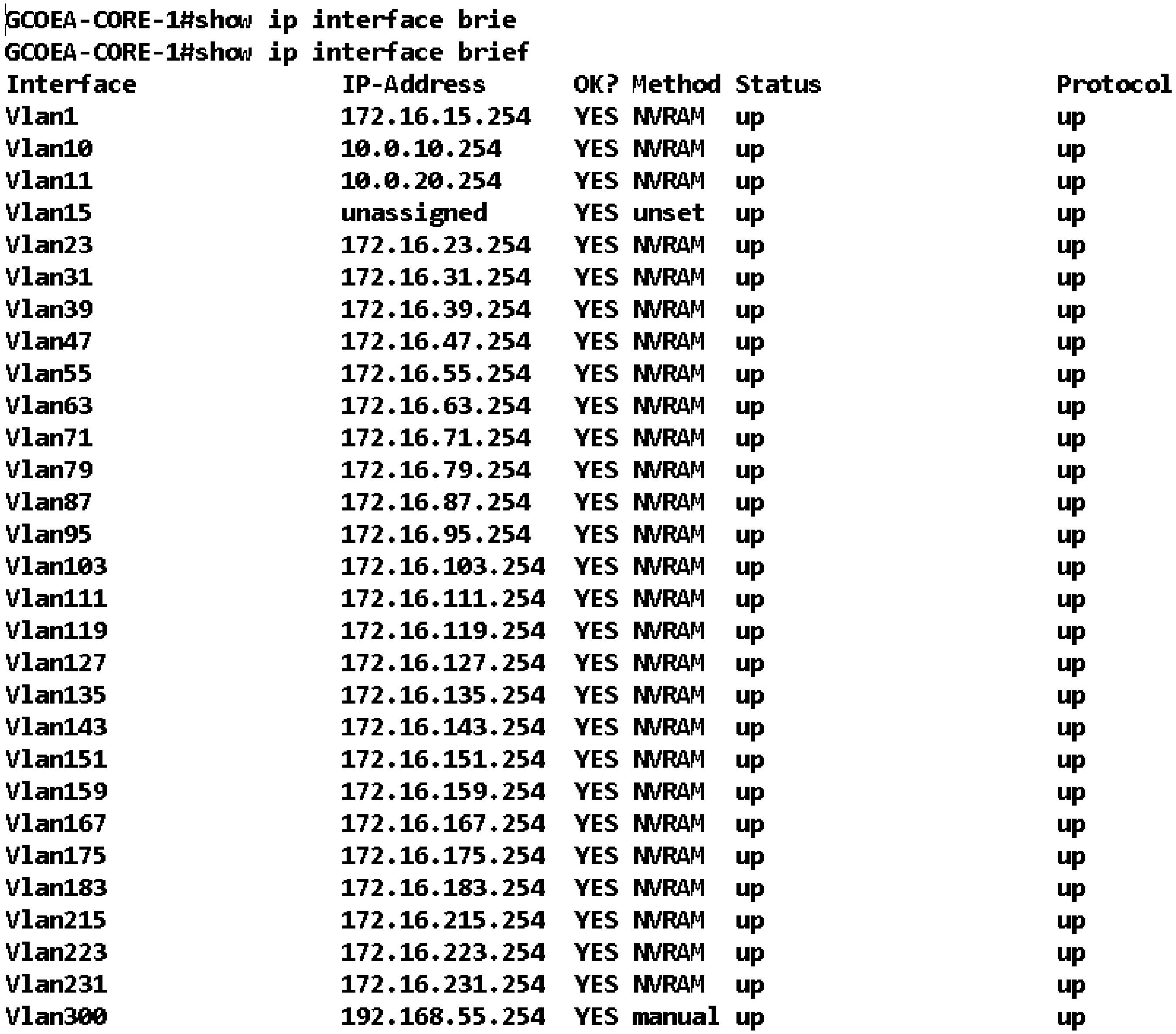
VLANs define broadcast domains in a Layer 2 network. A broadcast domain is the set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains are typically bounded by routers because routers do not forward broadcast frames. Layer 2 switches create broadcast domains based on the configuration of the switch. Switches are multiport bridges that allow you to create multiple broadcast domains. Each broadcast domain is like a distinct virtual bridge within a switch.



```
GCOEA-CORE-1#show vlan

VLAN Name                             Status
---- -------------------------------- --------
1    default                          active
10   VOICE_VLAN                       active
11   DATA_VLAN                        active
15   MANAGEMENT                       active
23   AP_MANAGEMENT                    active
31   SERVER                           active
39   FIREWALL                         active
47   VOICE                            active
55   ADMIN                            active
63   ELECTRICAL                       active
71   APPLIEDMECHANICS                 active
79   MECHANICAL                       active
87   CIVIL                            active
95   INSTRUMENTATION                  active
103  COMPUTER_ENGINEERING             active
111  GEOLOGY                          active
119  LIBRARY                          active
127  ELECTRONICS                      active
135  INFORMATION_TECH                 active
143  PHYSICS                          active
151  CHEMISTRY                        active
159  MATHAMATICS                      active
167  ADMINISTRATIVE_OFF               active
175  RAGISTAR                         active
183  WORKSHOP                         active
215  BOYS_HOSTEL_1                    active
223  STAFF_QTR                        active
231  GIRLS_HOSTEL                     active
300  NewServer                        active
```

Configuring Vlan Interfaces:

On creation of Vlan for different departments in the campus, next step is to give IP address to the configured Vlan. Refer chart for IP address set to different Vlan as below:



```
GCOEA-CORE-1#show ip interface brie
GCOEA-CORE-1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  172.16.15.254   YES NVRAM  up                    up
Vlan10                 10.0.10.254     YES NVRAM  up                    up
Vlan11                 10.0.20.254     YES NVRAM  up                    up
Vlan15                 unassigned      YES unset  up                    up
Vlan23                 172.16.23.254   YES NVRAM  up                    up
Vlan31                 172.16.31.254   YES NVRAM  up                    up
Vlan39                 172.16.39.254   YES NVRAM  up                    up
Vlan47                 172.16.47.254   YES NVRAM  up                    up
Vlan55                 172.16.55.254   YES NVRAM  up                    up
Vlan63                 172.16.63.254   YES NVRAM  up                    up
Vlan71                 172.16.71.254   YES NVRAM  up                    up
Vlan79                 172.16.79.254   YES NVRAM  up                    up
Vlan87                 172.16.87.254   YES NVRAM  up                    up
Vlan95                 172.16.95.254   YES NVRAM  up                    up
Vlan103                172.16.103.254  YES NVRAM  up                    up
Vlan111                172.16.111.254  YES NVRAM  up                    up
Vlan119                172.16.119.254  YES NVRAM  up                    up
Vlan127                172.16.127.254  YES NVRAM  up                    up
Vlan135                172.16.135.254  YES NVRAM  up                    up
Vlan143                172.16.143.254  YES NVRAM  up                    up
Vlan151                172.16.151.254  YES NVRAM  up                    up
Vlan159                172.16.159.254  YES NVRAM  up                    up
Vlan167                172.16.167.254  YES NVRAM  up                    up
Vlan175                172.16.175.254  YES NVRAM  up                    up
Vlan183                172.16.183.254  YES NVRAM  up                    up
Vlan215                172.16.215.254  YES NVRAM  up                    up
Vlan223                172.16.223.254  YES NVRAM  up                    up
Vlan231                172.16.231.254  YES NVRAM  up                    up
Vlan300                192.168.55.254  YES manual up                    up
```

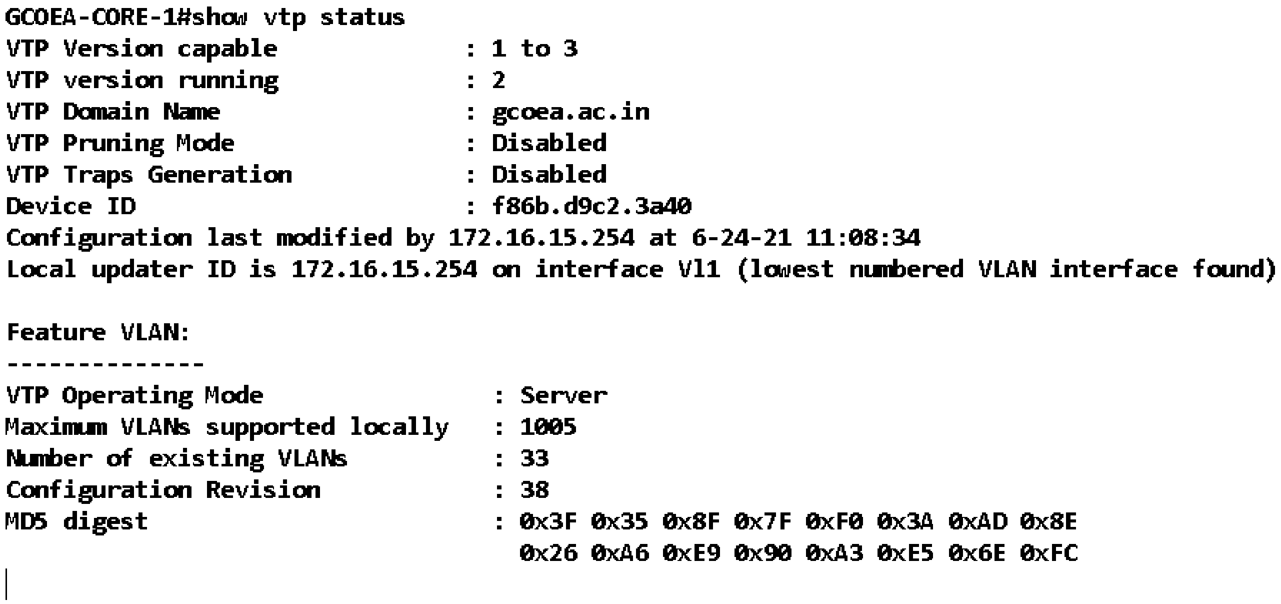
Configuring VTP and setting switch VTP mode as server:

Overview of VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches. VTP configuration information is saved in the VTP VLAN database. Catalyst switches can support VTP in one of three modes: Server, Client, and Transparent.

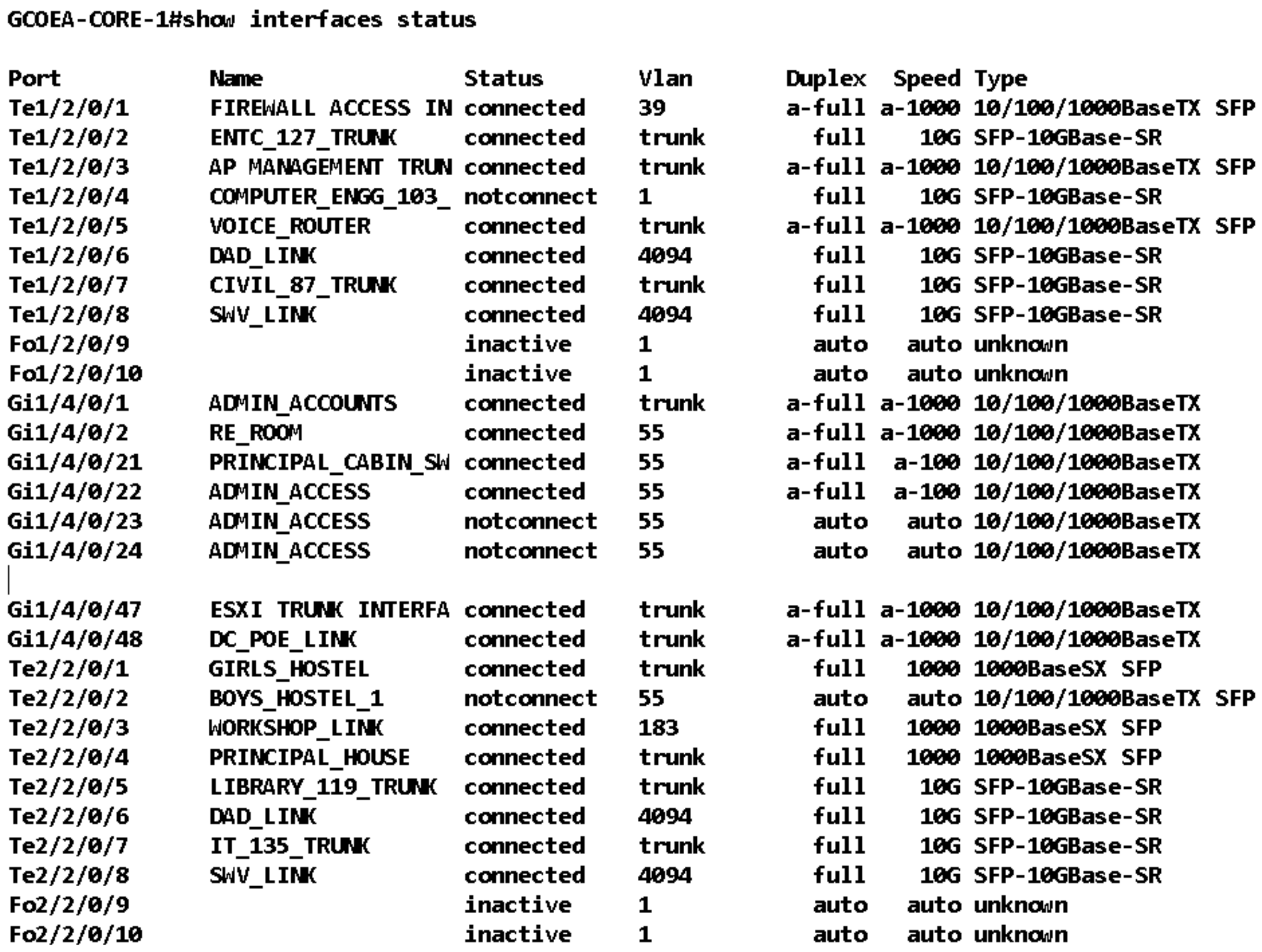
Server: Allows you to create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.



```
GCOEA-CORE-1#show vtp status
VTP Version capable              : 1 to 3
VTP version running              : 2
VTP Domain Name                  : gcoea.ac.in
VTP Pruning Mode                 : Disabled
VTP Traps Generation             : Disabled
Device ID                        : f86b.d9c2.3a40
Configuration last modified by 172.16.15.254 at 6-24-21 11:08:34
Local updater ID is 172.16.15.254 on interface Vl1 (lowest numbered VLAN interface found)

Feature VLAN:
--------------
VTP Operating Mode                 : Server
Maximum VLANs supported locally    : 1005
Number of existing VLANs           : 33
Configuration Revision             : 38
MD5 digest                         : 0x3F 0x35 0x8F 0x7F 0xF0 0x3A 0xAD 0x8E
                                     0x26 0xA6 0xE9 0x90 0xA3 0xE5 0x6E 0xFC
```

Assigning Ports to Vlan:

As mentioned Vlans are created to provide backbone connectivity to different department from datacenter in campus. Optic fiber cable 10G enabled network was deployed between datacenter to different departments. Switch stack interfaces can be configured in access or trunk mode. Departmental backbones are terminated to trunk interfaces and workstation etc in Admin Building of campus was termination to access interfaces. Please refer chart of active interface distribution as below:



```
GCOEA-CORE-1#show interfaces status

Port           Name               Status       Vlan       Duplex  Speed Type
Te1/2/0/1      FIREWALL ACCESS IN connected    39         a-full a-1000 10/100/1000BaseTX SFP
Te1/2/0/2      ENTC_127_TRUNK     connected    trunk        full    10G SFP-10GBase-SR
Te1/2/0/3      AP MANAGEMENT TRUN connected    trunk      a-full a-1000 10/100/1000BaseTX SFP
Te1/2/0/4      COMPUTER_ENGG_103_ notconnect   1            full    10G SFP-10GBase-SR
Te1/2/0/5      VOICE_ROUTER       connected    trunk      a-full a-1000 10/100/1000BaseTX SFP
Te1/2/0/6      DAD_LINK           connected    4094         full    10G SFP-10GBase-SR
Te1/2/0/7      CIVIL_87_TRUNK     connected    trunk        full    10G SFP-10GBase-SR
Te1/2/0/8      SWV_LINK           connected    4094         full    10G SFP-10GBase-SR
Fo1/2/0/9                         inactive     1            auto   auto unknown
Fo1/2/0/10                        inactive     1            auto   auto unknown
Gi1/4/0/1      ADMIN_ACCOUNTS     connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/4/0/2      RE_ROOM            connected    55         a-full a-1000 10/100/1000BaseTX
Gi1/4/0/21     PRINCIPAL_CABIN_SW connected    55         a-full  a-100 10/100/1000BaseTX
Gi1/4/0/22     ADMIN_ACCESS       connected    55         a-full  a-100 10/100/1000BaseTX
Gi1/4/0/23     ADMIN_ACCESS       notconnect   55           auto   auto 10/100/1000BaseTX
Gi1/4/0/24     ADMIN_ACCESS       notconnect   55           auto   auto 10/100/1000BaseTX
|
Gi1/4/0/47     ESXI TRUNK INTERFA connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/4/0/48     DC_POE_LINK        connected    trunk      a-full a-1000 10/100/1000BaseTX
Te2/2/0/1      GIRLS_HOSTEL       connected    trunk        full   1000 1000BaseSX SFP
Te2/2/0/2      BOYS_HOSTEL_1      notconnect   55           auto   auto 10/100/1000BaseTX SFP
Te2/2/0/3      WORKSHOP_LINK      connected    183          full   1000 1000BaseSX SFP
Te2/2/0/4      PRINCIPAL_HOUSE    connected    trunk        full   1000 1000BaseSX SFP
Te2/2/0/5      LIBRARY_119_TRUNK  connected    trunk        full    10G SFP-10GBase-SR
Te2/2/0/6      DAD_LINK           connected    4094         full    10G SFP-10GBase-SR
Te2/2/0/7      IT_135_TRUNK       connected    trunk        full    10G SFP-10GBase-SR
Te2/2/0/8      SWV_LINK           connected    4094         full    10G SFP-10GBase-SR
Fo2/2/0/9                         inactive     1            auto   auto unknown
Fo2/2/0/10                        inactive     1            auto   auto unknown
```

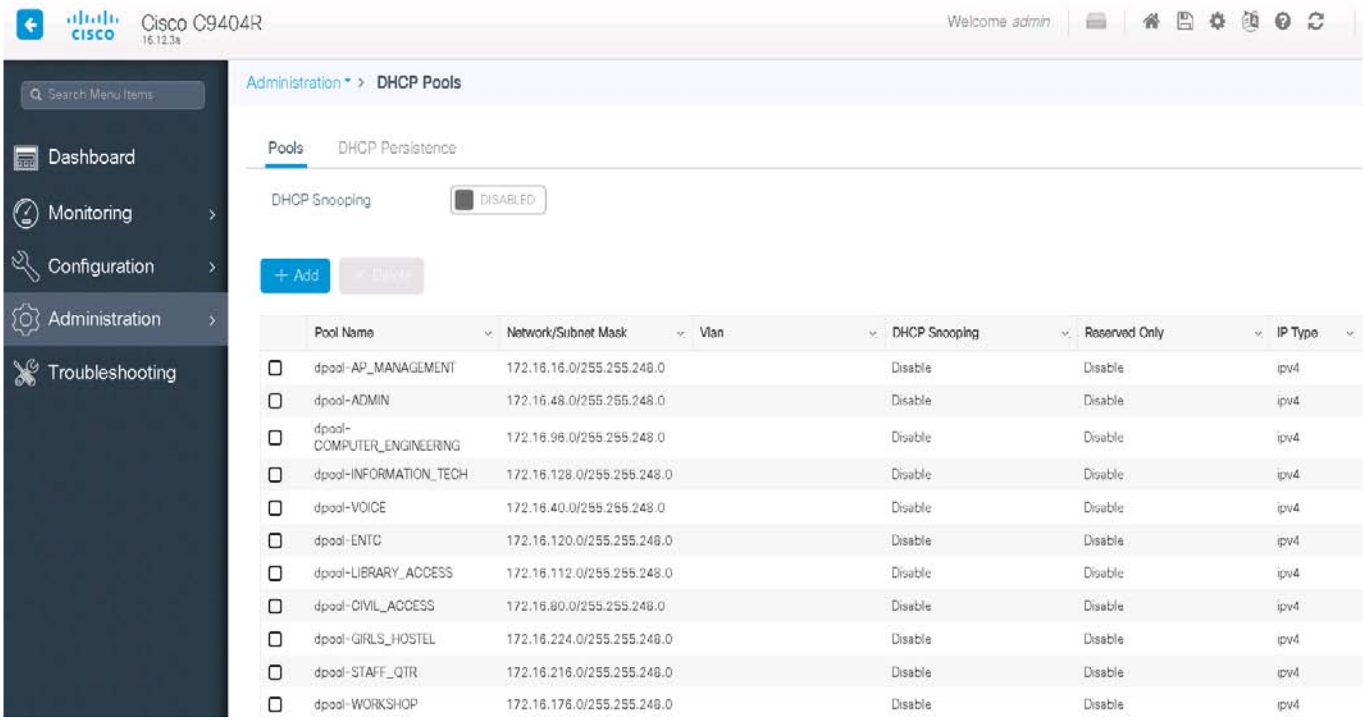
Configuring DHCP server for created Vlans:

Overview of the DHCP Server

The Cisco DHCP server accepts address assignment requests and renewals from the client and assigns the addresses from predefined groups of addresses within DHCP address pools. These address pools can also be configured to supply additional information to the requesting client such as the IP address of the Domain Name System (DNS) server, the default device, and other configuration parameters. The Cisco DHCP server can accept broadcasts from locally attached LAN segments or from DHCP requests that have been forwarded by other DHCP relay agents within the network.

Cisco devices running Cisco software include Dynamic Host Configuration Protocol (DHCP) server and the relay agent software. The Cisco IOS DHCP server is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the device to DHCP clients. The DHCP server can be configured to assign additional parameters such as the IP address of the Domain Name System (DNS) server and the default device.

In the switch stack we have configured the DHCP server for different departmental Vlan. Refer chart for configured DHCP server as below:

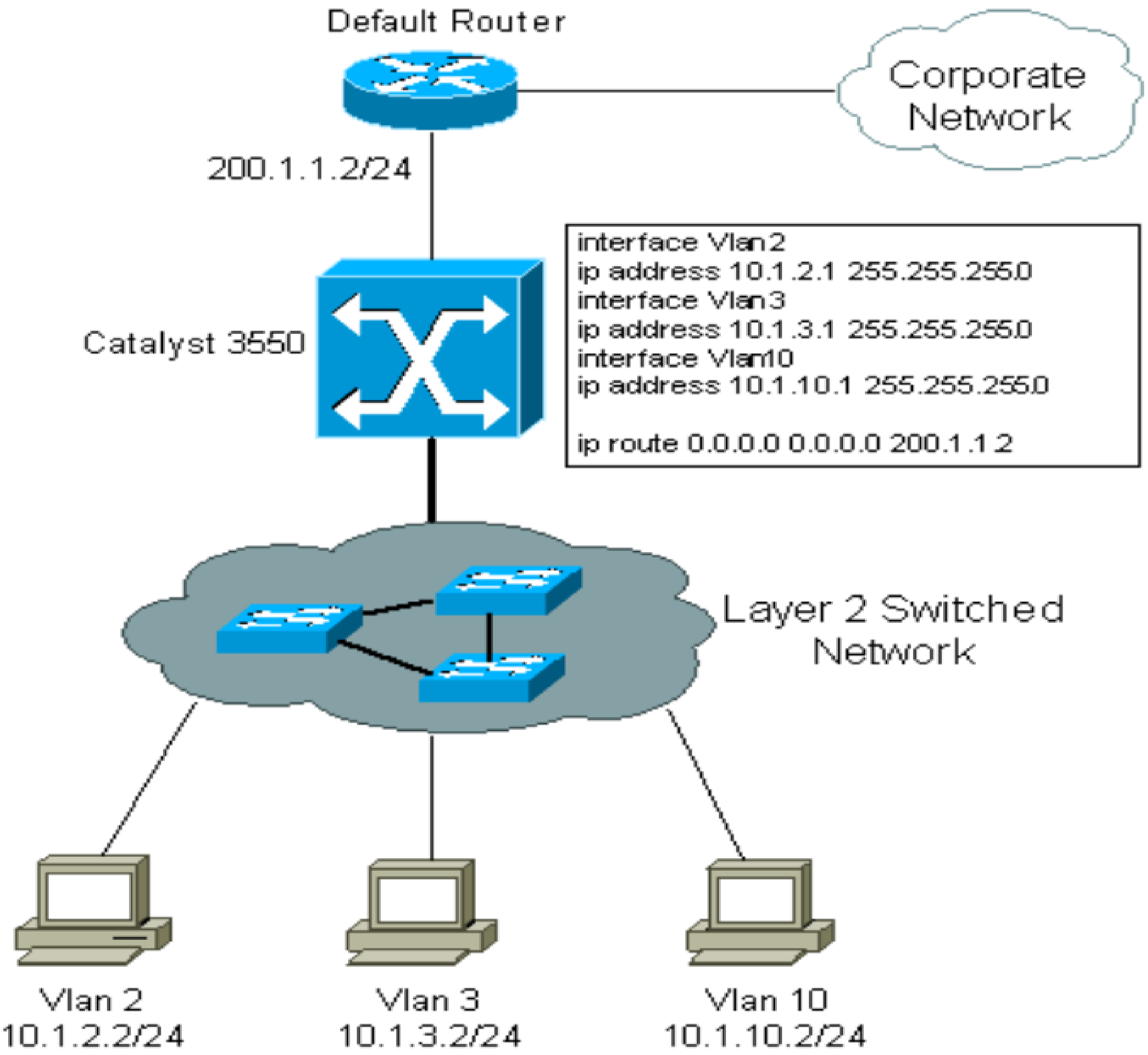


DHCP Snooping: DISABLED

	Pool Name	Network/Subnet Mask	Vlan	DHCP Snooping	Reserved Only	IP Type
□	dpool-AP_MANAGEMENT	172.16.16.0/255.255.248.0		Disable	Disable	ipv4
□	dpool-ADMIN	172.16.48.0/255.255.248.0		Disable	Disable	ipv4
□	dpool-COMPUTER_ENGINEERING	172.16.96.0/255.255.248.0		Disable	Disable	ipv4
□	dpool-INFORMATION_TECH	172.16.128.0/255.255.248.0		Disable	Disable	ipv4
□	dpool-VOICE	172.16.40.0/255.255.248.0		Disable	Disable	ipv4
□	dpool-ENTC	172.16.120.0/255.255.248.0		Disable	Disable	ipv4
□	dpool-LIBRARY_ACCESS	172.16.112.0/255.255.248.0		Disable	Disable	ipv4
□	dpool-CIVIL_ACCESS	172.16.80.0/255.255.248.0		Disable	Disable	ipv4
□	dpool-GIRLS_HOSTEL	172.16.224.0/255.255.248.0		Disable	Disable	ipv4
□	dpool-STAFF_QTR	172.16.216.0/255.255.248.0		Disable	Disable	ipv4
□	dpool-WORKSHOP	172.16.176.0/255.255.248.0		Disable	Disable	ipv4

Configuring Layer3 route:

Cisco IOS system software support InterVLAN routing features. We have configured the switch stack to forward traffic from all Vlan subnet to the firewall Cisco FPR2110 inside interface IP. The logical diagram of configuration is as below:



```
interface Vlan2
ip address 10.1.2.1 255.255.255.0
interface Vlan3
ip address 10.1.3.1 255.255.255.0
interface Vlan10
ip address 10.1.10.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0 200.1.1.2
```

****The actual Vlan and IP scheme vary*

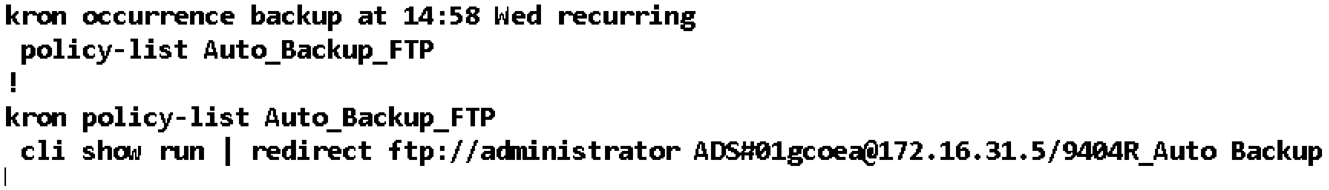
```
GCOEA-CORE-1#show ip route connected

Codes: L - local, C - connected,


Gateway of last resort is 172.16.39.253 to network 0.0.0.0


     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.0.10.0/24 is directly connected, Vlan10
L       10.0.10.254/32 is directly connected, Vlan10
C       10.0.20.0/24 is directly connected, Vlan11
L       10.0.20.254/32 is directly connected, Vlan11
     172.16.0.0/16 is variably subnetted, 50 subnets, 3 masks
C       172.16.8.0/21 is directly connected, Vlan1
L       172.16.15.254/32 is directly connected, Vlan1
C       172.16.16.0/21 is directly connected, Vlan23
L       172.16.23.254/32 is directly connected, Vlan23
C       172.16.24.0/21 is directly connected, Vlan31
L       172.16.31.254/32 is directly connected, Vlan31
C       172.16.39.248/29 is directly connected, Vlan39
L       172.16.39.254/32 is directly connected, Vlan39
C       172.16.40.0/21 is directly connected, Vlan47
L       172.16.47.254/32 is directly connected, Vlan47
C       172.16.48.0/21 is directly connected, Vlan55
L       172.16.55.254/32 is directly connected, Vlan55
C       172.16.56.0/21 is directly connected, Vlan63
L       172.16.63.254/32 is directly connected, Vlan63
```

```
C       172.16.64.0/21 is directly connected, Vlan71
L       172.16.71.254/32 is directly connected, Vlan71
C       172.16.72.0/21 is directly connected, Vlan79
L       172.16.79.254/32 is directly connected, Vlan79
C       172.16.80.0/21 is directly connected, Vlan87
L       172.16.87.254/32 is directly connected, Vlan87
C       172.16.88.0/21 is directly connected, Vlan95
L       172.16.95.254/32 is directly connected, Vlan95
C       172.16.96.0/21 is directly connected, Vlan103
L       172.16.103.254/32 is directly connected, Vlan103
C       172.16.104.0/21 is directly connected, Vlan111
L       172.16.111.254/32 is directly connected, Vlan111
C       172.16.112.0/21 is directly connected, Vlan119
L       172.16.119.254/32 is directly connected, Vlan119
C       172.16.120.0/21 is directly connected, Vlan127
L       172.16.127.254/32 is directly connected, Vlan127
C       172.16.128.0/21 is directly connected, Vlan135
L       172.16.135.254/32 is directly connected, Vlan135
C       172.16.136.0/21 is directly connected, Vlan143
L       172.16.143.254/32 is directly connected, Vlan143
C       172.16.144.0/21 is directly connected, Vlan151
L       172.16.151.254/32 is directly connected, Vlan151
C       172.16.152.0/21 is directly connected, Vlan159
L       172.16.159.254/32 is directly connected, Vlan159
C       172.16.160.0/21 is directly connected, Vlan167
L       172.16.167.254/32 is directly connected, Vlan167
```

```
C        172.16.168.0/21 is directly connected, Vlan175

L        172.16.175.254/32 is directly connected, Vlan175

C        172.16.176.0/21 is directly connected, Vlan183

L        172.16.183.254/32 is directly connected, Vlan183

C        172.16.208.0/21 is directly connected, Vlan215

L        172.16.215.254/32 is directly connected, Vlan215

C        172.16.216.0/21 is directly connected, Vlan223

L        172.16.223.254/32 is directly connected, Vlan223

C        172.16.224.0/21 is directly connected, Vlan231

L        172.16.231.254/32 is directly connected, Vlan231

     192.168.55.0/24 is variably subnetted, 2 subnets, 2 masks

C        192.168.55.0/24 is directly connected, Vlan300

L        192.168.55.254/32 is directly connected, Vlan300
```

Configuring auto backup of switch stack running configuration:

Cisco switch configuration backups. Solution: Cisco KRON via CLI The Cisco KRON is a command scheduler utility. It allows you to schedule commands to run once, at system startup, or at specified dates and times. Refer status of auto backup configured as below:



```
kron occurrence backup at 14:58 Wed recurring
 policy-list Auto_Backup_FTP
!
kron policy-list Auto_Backup_FTP
 cli show run | redirect ftp://administrator ADS#01gcoea@172.16.31.5/9404R_Auto Backup
```

Configuring SNMP:

Overview of SNMP

Simple Network Management Protocol (SNMP) is a way for different devices on a network to share information with one another. It allows devices to communicate even if the devices are different hardware and run different software.

Without a protocol like SNMP, there would be no way for network management tools to identify devices, monitor network performance, keep track of changes to the network, or determine the status of network devices in real time.

SNMPv3

SNMPv3 makes data encryption possible. It also allows admins to specify different authentication requirements on a granular basis for managers and agents. This prevents unauthorized authentication and can optionally be used to require encryption for data transfers.

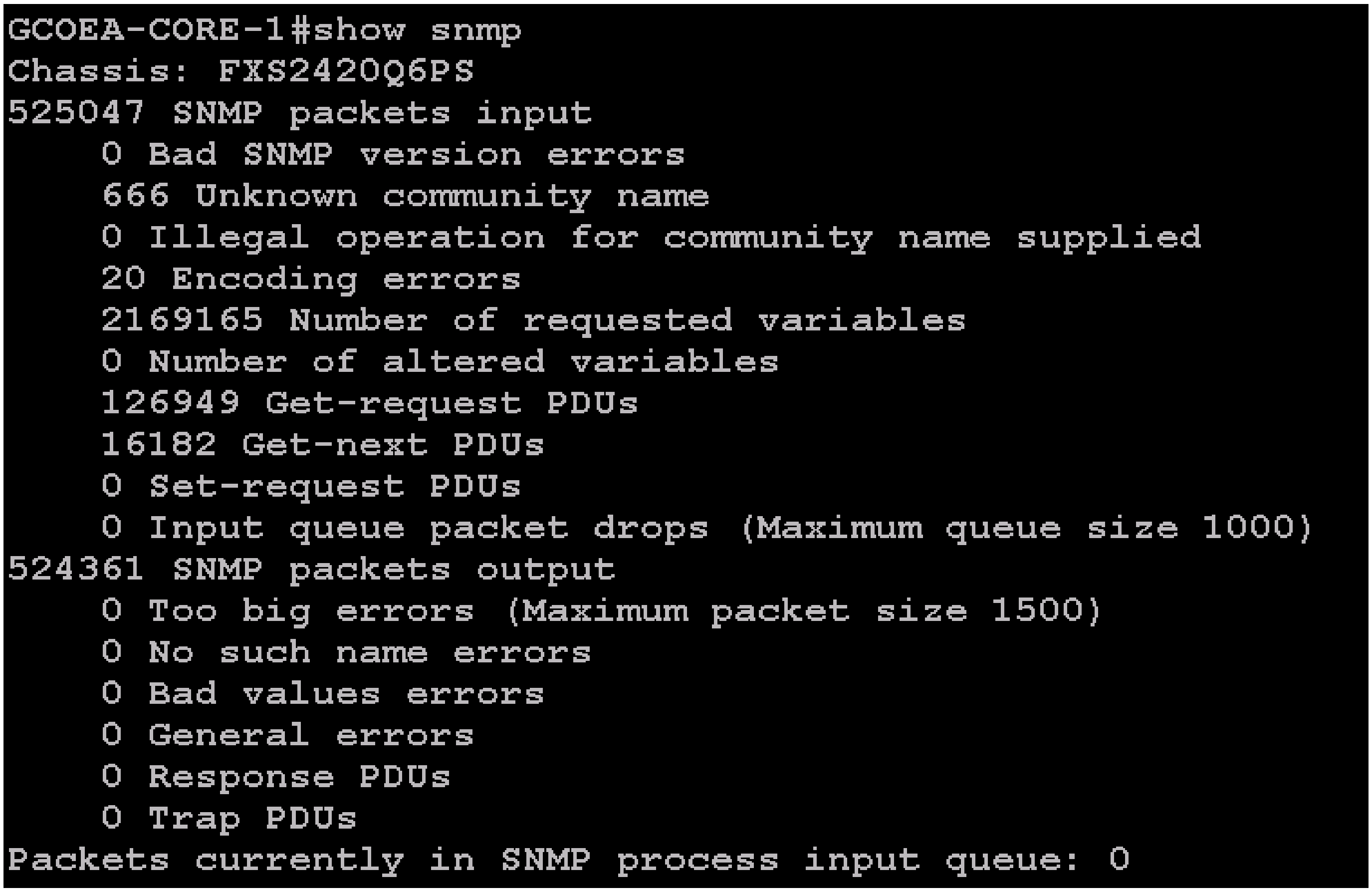
The bottom line is that, while the security issues in SNMPv1 earned SNMP a bad name in some circles, SNMPv2 and especially SNMPv3 solved those problems. The newer versions of SNMP provide an up-to-date, secure way to monitor the network.

The SNMP Version 3 feature provides secure access to devices by authenticating and encrypting data packets over the network. Simple Network Management Protocol version 3 (SNMPv3) is an interoperable, standards-based protocol that is defined in RFCs 3413 to 3415.

SNMPv3 is a security model in which an authentication strategy is set up for a user and the group in which the user resides. Security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used when handling an SNMP packet.

In deployed network devices in Campus we have configured SNMPv3. SNMPv3 is used to establish communication between network devices and Prime Infrastructure Network Management Software installed in the virtualized server in datacenter.

Refer SNMP status as below;



```
GCOEA-CORE-1#show snmp
Chassis: FXS2420Q6PS
525047 SNMP packets input
    0 Bad SNMP version errors
    666 Unknown community name
    0 Illegal operation for community name supplied
    20 Encoding errors
    2169165 Number of requested variables
    0 Number of altered variables
    126949 Get-request PDUs
    16182 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
524361 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
Packets currently in SNMP process input queue: 0
```

*****Apart for above config we have added FTP server, enabled GUI access of switch stack and login banner etc.**

Cisco C9200L-24P-4x-E Catalyst 9200L 24-port POE+, 4 x 10G

Extend intent-based networking everywhere

Cisco® Catalyst® 9200 Series switches extend the power of intent-based networking and Catalyst 9000 hardware and software innovation to a broader set of deployments. With its family pedigree, **Catalyst 9200 Series switches offer simplicity without compromise – it is secure, always on, and IT simplified.**

As foundational building blocks for the Cisco Digital Network Architecture, Catalyst 9200 Series switches help customers simplify complexity, optimize IT, and reduce operational costs by leveraging intelligence, automation and human expertise that no other vendor can deliver regardless of where you are in the intent-based networking journey.

Catalyst 9200 Series switches provide security features that protect the integrity of the hardware as well as the software and all data that flows through the switch. It provides resiliency that keeps your business up and running seamlessly. Combine that with open APIs of Cisco IOS XE and programmability of the UADP ASIC technology, Catalyst 9200 Series switches give you what you need now with investment protection on future innovations.

With full PoE+ capability, power and fan redundancy, stacking bandwidth up to 160 Gbps, modular uplinks, Layer 3 feature support, and cold patching, Catalyst 9200 Series switches are the industry's unparalleled solution with differentiated resiliency and progressive architecture for cost-effective branch-office access.

Bandwidth specifications

Description	Switching capacity	Switch capacity with Stacking	Forwarding rate	Forwarding rate with Stacking
C9200L-24P-4X	128 Gbps	208 Gbps	95.23 Mpps	155 Mpps

Cisco Catalyst 9200 Series Switch configurations

Switch model	Downlinks total 10/100/1000 or PoE+ copper ports	Uplink configuration	Default primary AC power supply	Fans
C9200L-24P-4X	24 ports full PoE+	4x 1/10G fixed uplinks	PWR-C5-600WAC	Fixed redundant

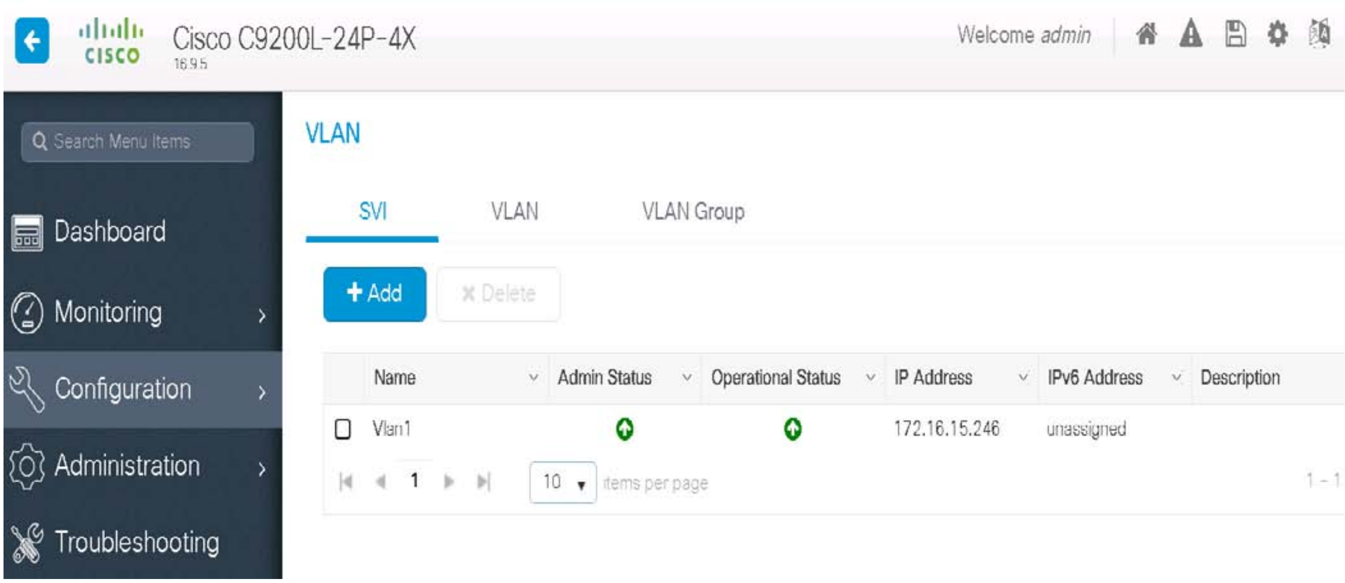
Cisco C9200L-24P-4x-E Deployment Includes:

- Configuring management interface
- Configuring the ip domain name, ip name-servers and NTP server
- Registration of switch for DNA licensing using Cisco Smart Licensing Portal
- Formation of Vlans
- Configuring VTP and setting switch VTP mode as server
- Configuring Vlan interfaces
- Assigning ports to Vlans
- Configuring DHCP server for created Vlans, exclusion of IP address for static use
- Configuring layer3 route
- Configuring auto backup of switch stack running configuration for disaster recovery
- Enabling switch stack GUI access
- Assigning banner to switch stack

Configuring management interface:

- To manage the Cisco switch, we need to configure a management interface. Unlike the routers that allow for management on any configured interface.
- The configured management interface of C9404R is as below:

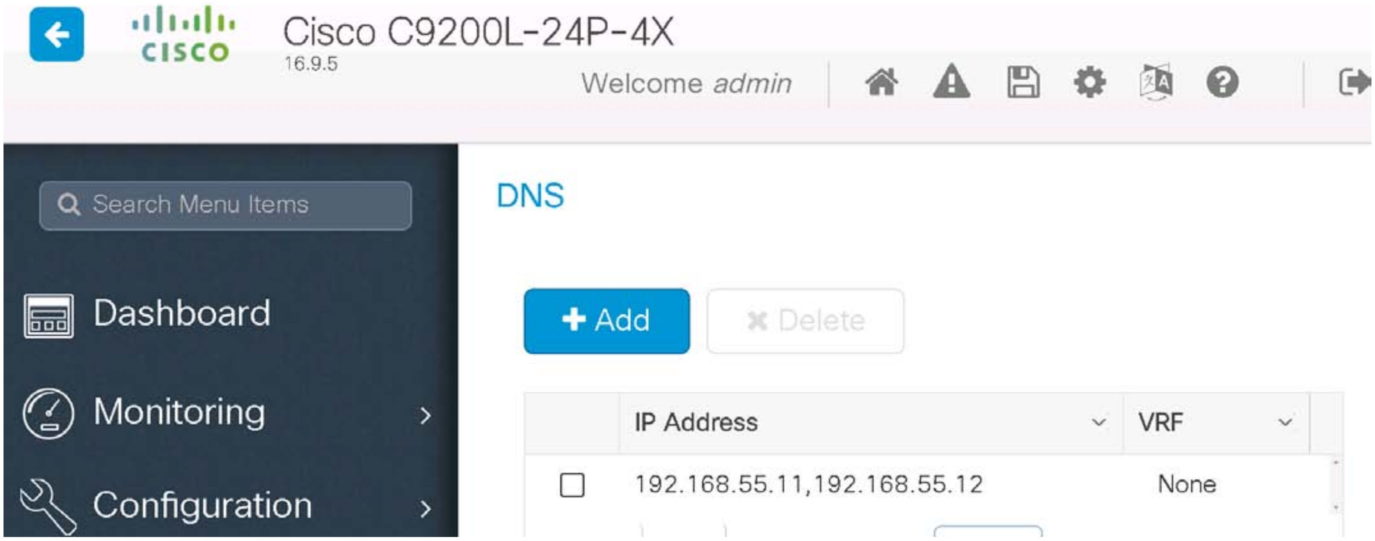
```
CIVIL_ACCESS#show run int vlan 1

Building configuration...
Current configuration : 63 bytes
interface Vlan1
 ip address 172.16.15.246 255.255.248.0
end
```



	Name	Admin Status	Operational Status	IP Address	IPv6 Address	Description
□	Vlan1	●	●	172.16.15.246	unassigned	

Configuring the ip domain name, ip name servers and NTP server

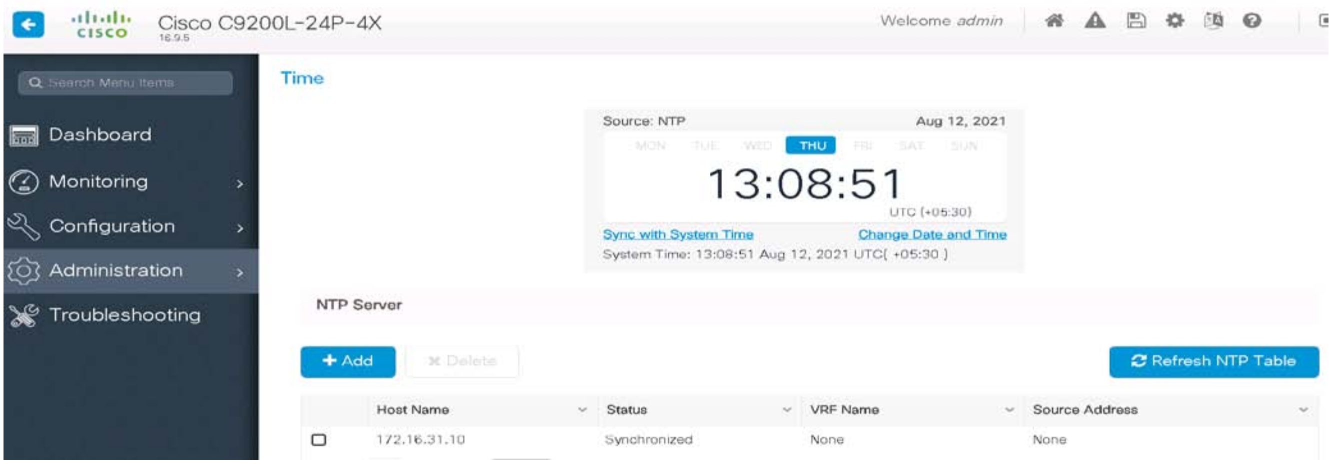
To provide redundancy we have configured primary and secondary domain controller in the data center. The both domain controllers are hosted as a guest in virtualized environment in the datacenter. Presently the domain controllers are not kept in production as the uptime is not guaranteed as the old HP server on which the domain controllers are hosted auto restart frequently. The active directory domain service users and computer details for staff, faculty and student was not yet made available by the college. Refer image as below for configured domain controllers:



DNS

	IP Address	VRF
□	192.168.55.11,192.168.55.12	None

Network Time Protocol server is running on a Windows server in datacenter. It is applied to the network appliance switches WLC, Vmware servers etc, which acquires and uses time from an NTP configured on Windows server in datacenter to maintain time within its local internal clock, and then supply the time to its connected network. This is achieved using the NTP or Network Time Protocol.



Time

Source: NTP Aug 12, 2021

13:08:51
UTC (+05:30)

System Time: 13:08:51 Aug 12, 2021 UTC(+05:30)

NTP Server

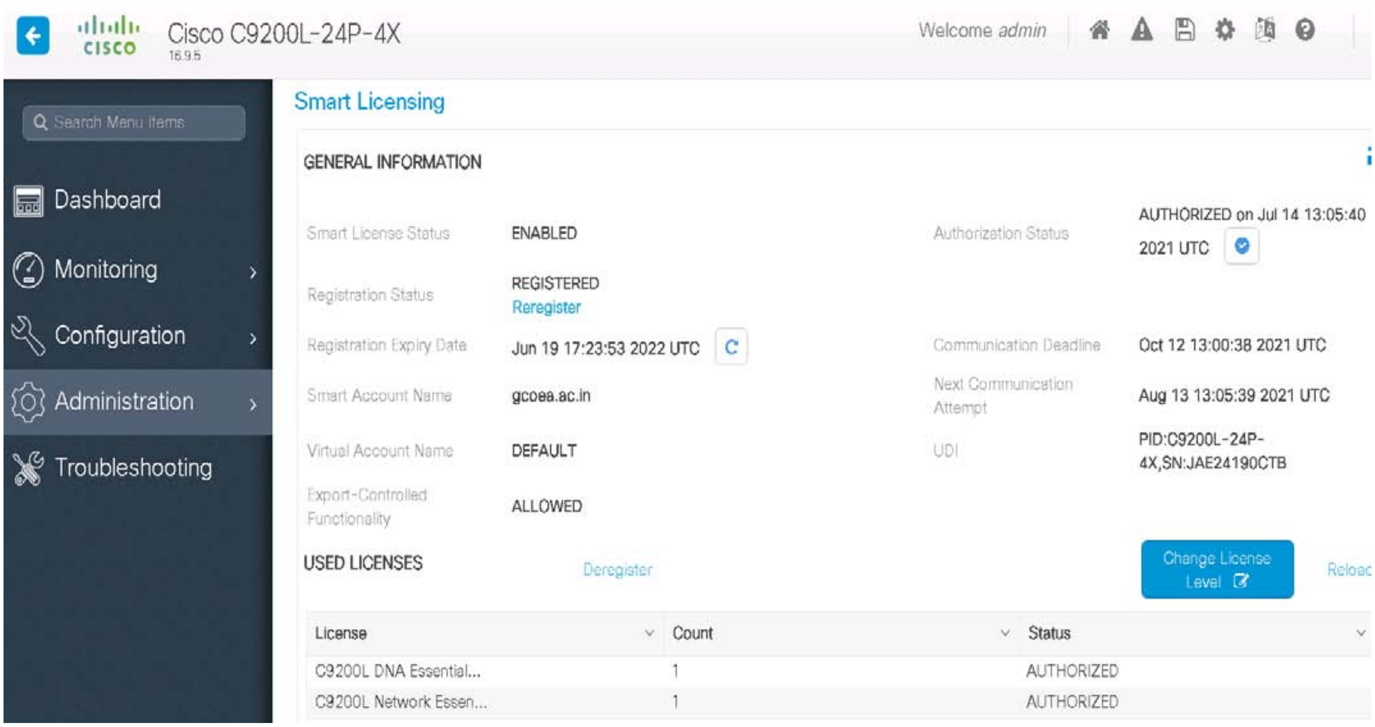
	Host Name	Status	VRF Name	Source Address
□	172.16.31.10	Synchronized	None	None

Registration of switch stack for DNA licensing using Cisco Smart Software Licensing Portal:

Information about Smart Licensing

Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends. Smart Licensing helps simplify three core functions:

- Purchasing
- Management
- Reporting



Smart Licensing

GENERAL INFORMATION

Smart License Status: ENABLED

Authorization Status: AUTHORIZED on Jul 14 13:05:40 2021 UTC

Registration Status: REGISTERED

Registration Expiry Date: Jun 19 17:23:53 2022 UTC

Communication Deadline: Oct 12 13:00:38 2021 UTC

Smart Account Name: gcoea.ac.in

Next Communication Attempt: Aug 13 13:05:39 2021 UTC

Virtual Account Name: DEFAULT

UDI: PID:C9200L-24P-4X,SN:JAE24190CTB

Export-Controlled Functionality: ALLOWED

USED LICENSES

License	Count	Status
C9200L DNA Essential...	1	AUTHORIZED
C9200L Network Essen...	1	AUTHORIZED

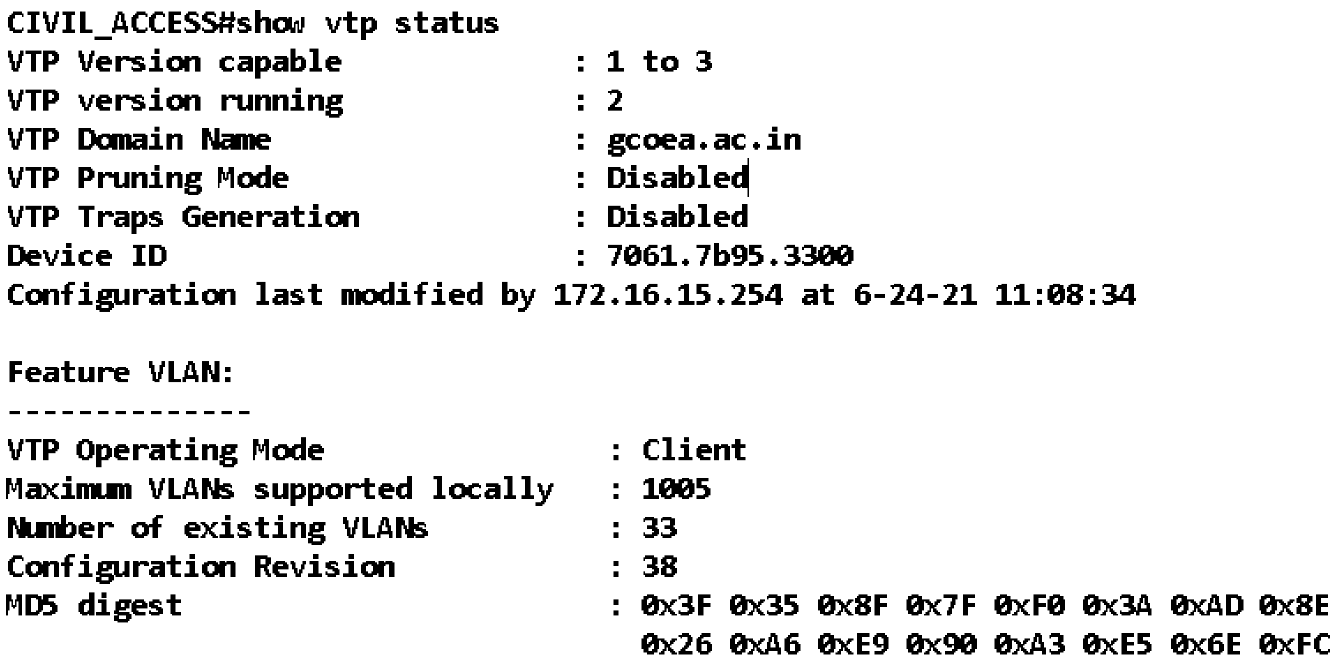
Configuring VTP and setting switch VTP mode as client:

Overview of VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches. VTP configuration information is saved in the VTP VLAN database. Catalyst switches can support VTP in one of three modes: Server, Client, and Transparent.

Server: Chassis switch stack the core switch of the network is configured as VTP mode server and all distribution and access switches are configured as VTP mode client. Refer Image below of configured VTP mode on distribution or access switches:

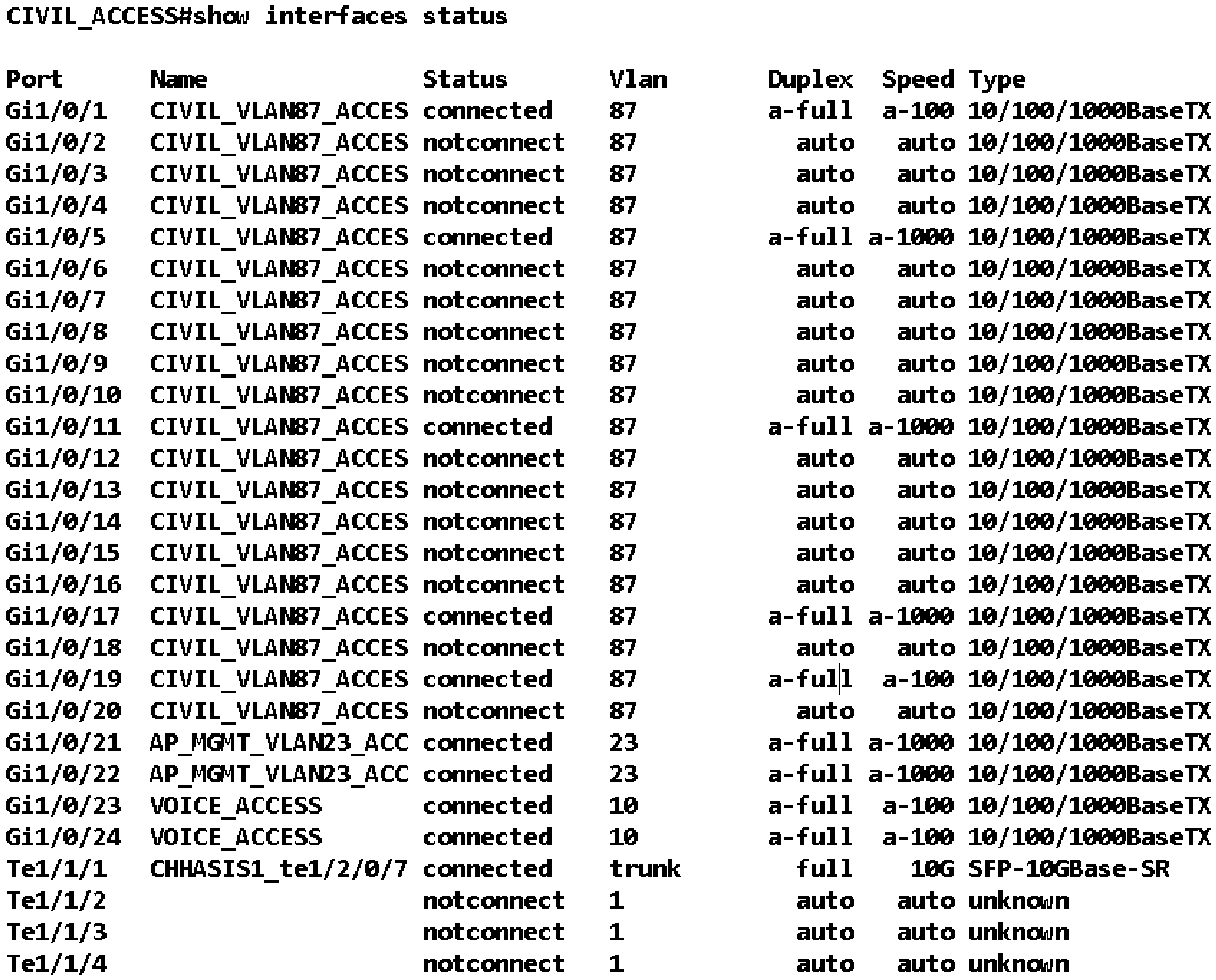


```
CIVIL_ACCESS#show vtp status
VTP Version capable                : 1 to 3
VTP version running                : 2
VTP Domain Name                    : gcoea.ac.in
VTP Pruning Mode                   : Disabled
VTP Traps Generation               : Disabled
Device ID                          : 7061.7b95.3300
Configuration last modified by 172.16.15.254 at 6-24-21 11:08:34

Feature VLAN:
--------------
VTP Operating Mode                   : Client
Maximum VLANs supported locally      : 1005
Number of existing VLANs             : 33
Configuration Revision               : 38
MD5 digest                           : 0x3F 0x35 0x8F 0x7F 0xF0 0x3A 0xAD 0x8E
                                       0x26 0xA6 0xE9 0x90 0xA3 0xE5 0x6E 0xFC
```

Assigning Ports to Vlan:

As the switch is configured in VTP client mode all the Vlans configured in Core chassis switch in datacenter gets automatically populated in tjis switch. The trunk link from the Core chassis switch was connected on Te1/0/1 interface over 10G link. Interfaces Gi1/0/1 to Gi1/0/20 was configured in access mode accessing Vlan 87of Civil Department switch.

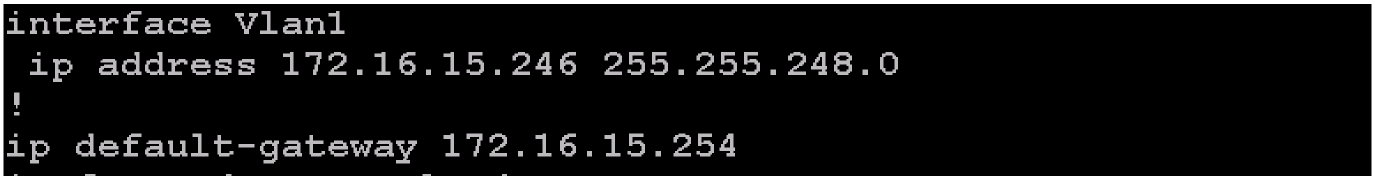
Please refer chart of interface distribution as below:



```
CIVIL_ACCESS#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1   CIVIL_VLAN87_ACCES connected    87         a-full  a-100 10/100/1000BaseTX
Gi1/0/2   CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/3   CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/4   CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/5   CIVIL_VLAN87_ACCES connected    87         a-full a-1000 10/100/1000BaseTX
Gi1/0/6   CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/7   CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/8   CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/9   CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/10  CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/11  CIVIL_VLAN87_ACCES connected    87         a-full a-1000 10/100/1000BaseTX
Gi1/0/12  CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/13  CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/14  CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/15  CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/16  CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/17  CIVIL_VLAN87_ACCES connected    87         a-full a-1000 10/100/1000BaseTX
Gi1/0/18  CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/19  CIVIL_VLAN87_ACCES connected    87         a-full  a-100 10/100/1000BaseTX
Gi1/0/20  CIVIL_VLAN87_ACCES notconnect   87           auto   auto 10/100/1000BaseTX
Gi1/0/21  AP_MGMT_VLAN23_ACC connected    23         a-full a-1000 10/100/1000BaseTX
Gi1/0/22  AP_MGMT_VLAN23_ACC connected    23         a-full a-1000 10/100/1000BaseTX
Gi1/0/23  VOICE_ACCESS       connected    10         a-full  a-100 10/100/1000BaseTX
Gi1/0/24  VOICE_ACCESS       connected    10         a-full  a-100 10/100/1000BaseTX
Te1/1/1   CHHASIS1_te1/2/0/7 connected    trunk        full    10G SFP-10GBase-SR
Te1/1/2                      notconnect   1            auto   auto unknown
Te1/1/3                      notconnect   1            auto   auto unknown
Te1/1/4                      notconnect   1            auto   auto unknown
```

Configuring Layer2 Default Gateway:

The switch is configured with a default gateway forwarding all traffic from Civil Department Vlan 87 to the Core chassis switch stack in datacenter. The configuration is as below:



```
interface Vlan1
 ip address 172.16.15.246 255.255.248.0
!
ip default-gateway 172.16.15.254
```

Configuring SNMP:

Overview of SNMP

Simple Network Management Protocol (SNMP) is a way for different devices on a network to share information with one another. It allows devices to communicate even if the devices are different hardware and run different software.

Without a protocol like SNMP, there would be no way for network management tools to identify devices, monitor network performance, keep track of changes to the network, or determine the status of network devices in real time.

SNMPv3

SNMPv3 makes data encryption possible. It also allows admins to specify different authentication requirements on a granular basis for managers and agents. This prevents unauthorized authentication and can optionally be used to require encryption for data transfers.

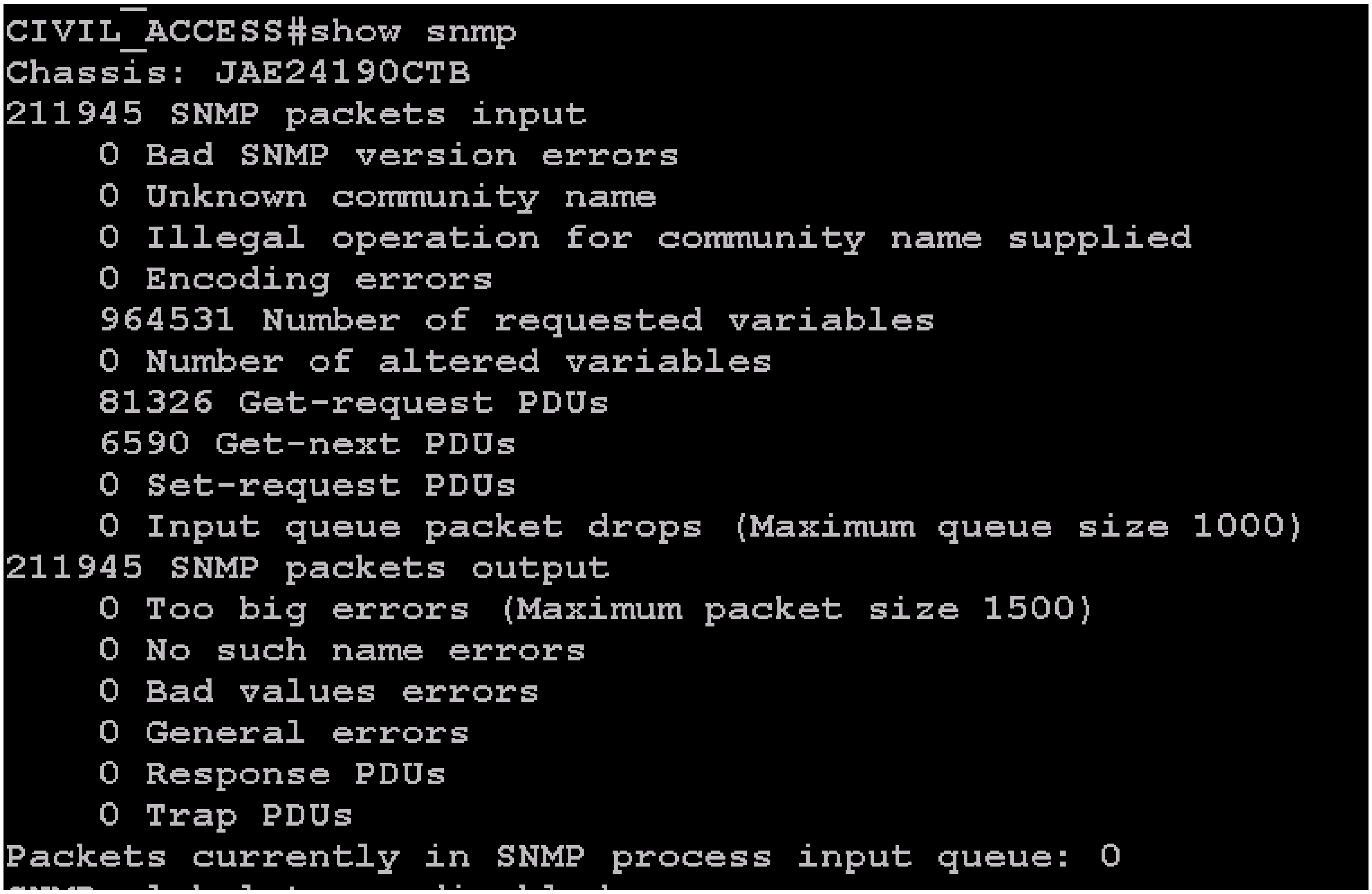
The bottom line is that, while the security issues in SNMPv1 earned SNMP a bad name in some circles, SNMPv2 and especially SNMPv3 solved those problems. The newer versions of SNMP provide an up-to-date, secure way to monitor the network.

The SNMP Version 3 feature provides secure access to devices by authenticating and encrypting data packets over the network. Simple Network Management Protocol version 3 (SNMPv3) is an interoperable, standards-based protocol that is defined in RFCs 3413 to 3415.

SNMPv3 is a security model in which an authentication strategy is set up for a user and the group in which the user resides. Security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used when handling an SNMP packet.

In deployed network devices in Campus we have configured SNMPv3. SNMPv3 is used to establish communication between network devices and Prime Infrastructure Network Management Software installed in the virtualized server in datacenter.

Refer SNMP status as below:

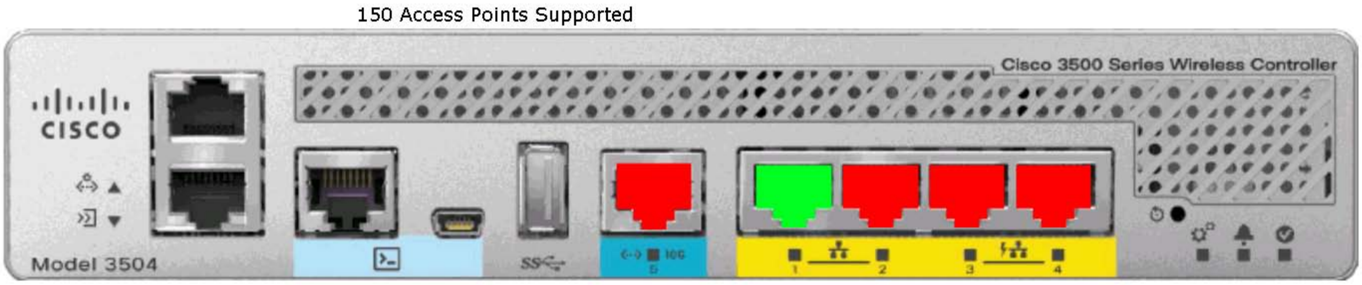


```
CIVIL_ACCESS#show snmp
Chassis: JAE24190CTB
211945 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    964531 Number of requested variables
    0 Number of altered variables
    81326 Get-request PDUs
    6590 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
211945 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
Packets currently in SNMP process input queue: 0
```

*****Apart for above config we have added FTP server, enabled GUI access of switch stack and login banner etc.**

*****All the switches Cisco C9200L-24P-4G-E Catalyst 9200L 24-port PoE+, 4 x 1G Cisco C9200L-24P-4X-E Catalyst 9200L 24-port PoE+, 4 x 10G are configured as described above. The management IP and backbone fiber connectivity speed of switches differ.**

***** All the existing network switches installed in different departments are connected to the installed new access switches.**


150 Access Points Supported
Cisco 3500 Series Wireless Controller
CISCO
Model 3504

Cisco 3504 Wireless Controller

Product overview

The Cisco 3504 Wireless Controller provides centralized control, management, and troubleshooting for small to medium-sized enterprises and branch offices. It offers flexibility to support multiple deployment modes in the same controller—a centralized mode for campus environments, Cisco FlexConnect® mode for lean branches managed over the WAN, and a mesh (bridge) mode for deployments in which full Ethernet cabling is unavailable. As a component of the Cisco Unified Wireless Network, the 3504 controller provides real-time communications between Cisco Aironet® access points and Cisco Catalyst® access points Cisco Prime® Infrastructure, and the Cisco Mobility Services Engine, and is interoperable with the Cisco 5520 and 8540 Wireless Controllers.

Product specifications

Item	Specifications
Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave 1 and Wave 2, Wi-Fi 6 (802.11ax)
Management interfaces	● Web-based: HTTP/HTTPS ● Command-line interface: Telnet, Secure Shell (SSH) Protocol, serial port ● Cisco Prime Infrastructure
Interfaces and indicators	● 1x Multigigabit Ethernet interface (up to 5 Gigabit Ethernet) + 4x 1 Gigabit Ethernet interfaces (RJ-45) ● 1x service port: 1 Gigabit Ethernet port (RJ-45) ● 1x redundancy port: 1 Gigabit Ethernet port (RJ-45) ● 1x console port: Serial port (RJ-45) ● 1x console port: Serial port (mini-B USB) ● 1x USB 3.0 port ● LED indicators: Network link, diagnostics

Cisco 3504 Wireless Controller Deployment Includes:

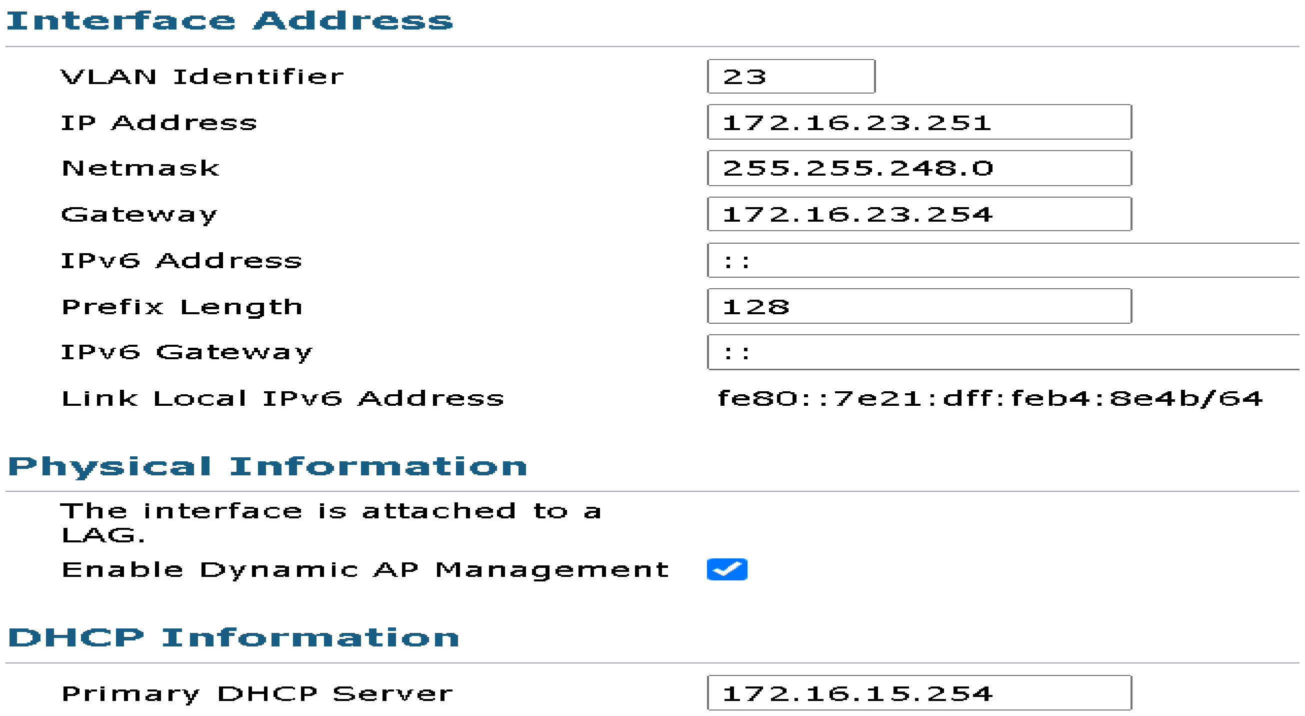
- Configuring dynamic AP Management Interface
- Configuring NTP server
- Discovery of access points on wireless controller
- Configuring user interface
- Configuring SSID
- On boarding of clients
- Monitoring

Configuring dynamic AP management Interface:

Management Interface

The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. It is also used for communications between the controller and access points, for all CAPWAP or intercontroller mobility messaging and tunneling traffic. You can access the GUI of the controller by entering the management interface IP address of the controller in the address field of your browser. The AP management is enabled by default on the management interface.

For CAPWAP, the controller requires one management interface to control all inter-controller communications and one AP-manager interface to control all controller-to-access point communications, regardless of the number of ports.



Interface Address

VLAN Identifier	23
IP Address	172.16.23.251
Netmask	255.255.248.0
Gateway	172.16.23.254
IPv6 Address	::
Prefix Length	128
IPv6 Gateway	::
Link Local IPv6 Address	fe80::7e21:dff:feb4:8e4b/64

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management	☑

DHCP Information

Primary DHCP Server	172.16.15.254

Discovery of access points on wireless controller

Overview of the Wireless LAN Controller (WLC) Discovery and Join Process

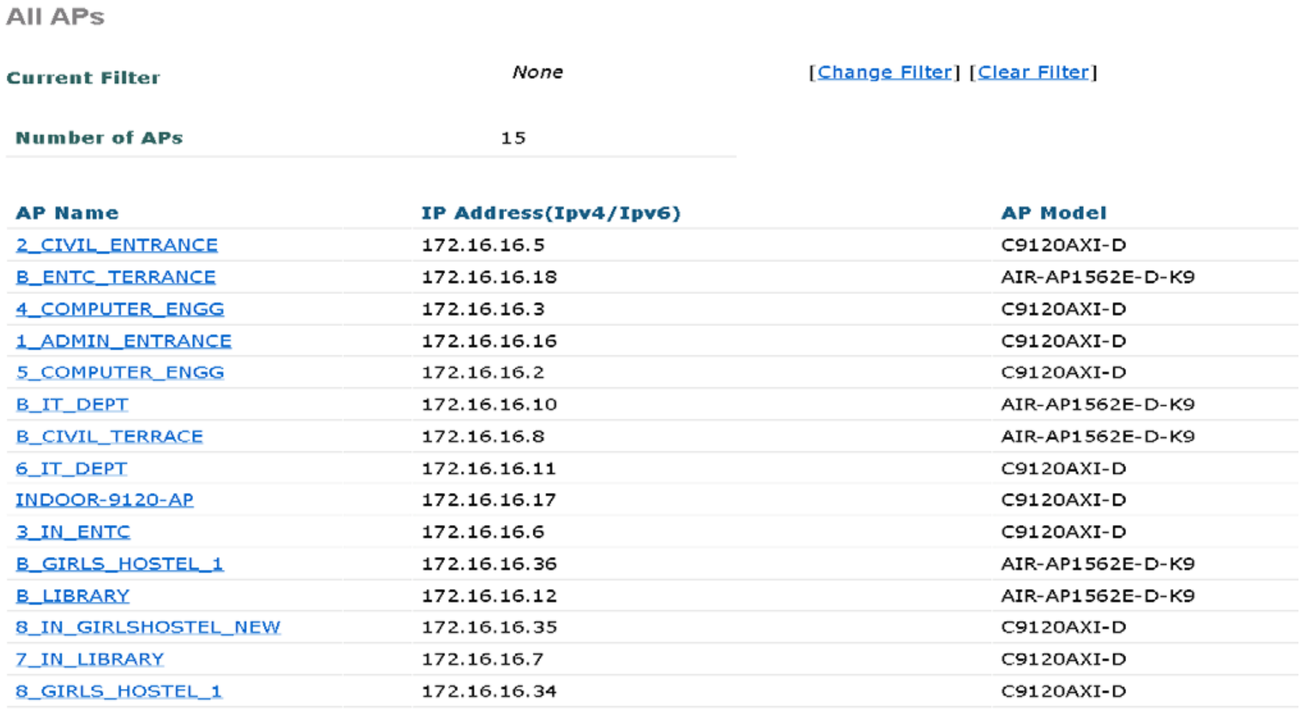
In a Cisco Unified Wireless network, the LAPs must first discover and join a WLC before they can service wireless clients.

However, this presents a question: how did the LAPs find the management IP address of the controller when it is on a different subnet?

If you do not tell the LAP where the controller is via DHCP option 43, DNS resolution of "Cisco-capwap-controller.local_domain", or statically configure it, the LAP does not know where in the network to find the management interface of the controller.

In addition to these methods, the LAP does automatically look on the local subnet for controllers with a 255.255.255.255 local broadcast. Also, the LAP remembers the management IP address of any controller it joins across reboots. Therefore, if you put the LAP first on the local subnet of the management interface, it will find the controller's management interface and remember the address. This is called priming. This does not help find the controller if you replace a LAP later on. Therefore, Cisco recommends using the DHCP option 43 or DNS methods.

The LAPs always connect to the management interface address of the controller first with a discovery request. The controller then tells the LAP the Layer 3 AP-manager interface (which can also be the management by default)IP address so the LAP can send a join request to the AP-manager interface next.



All APs

Current Filter	None	[Change Filter] [Clear Filter]
Number of APs	15	

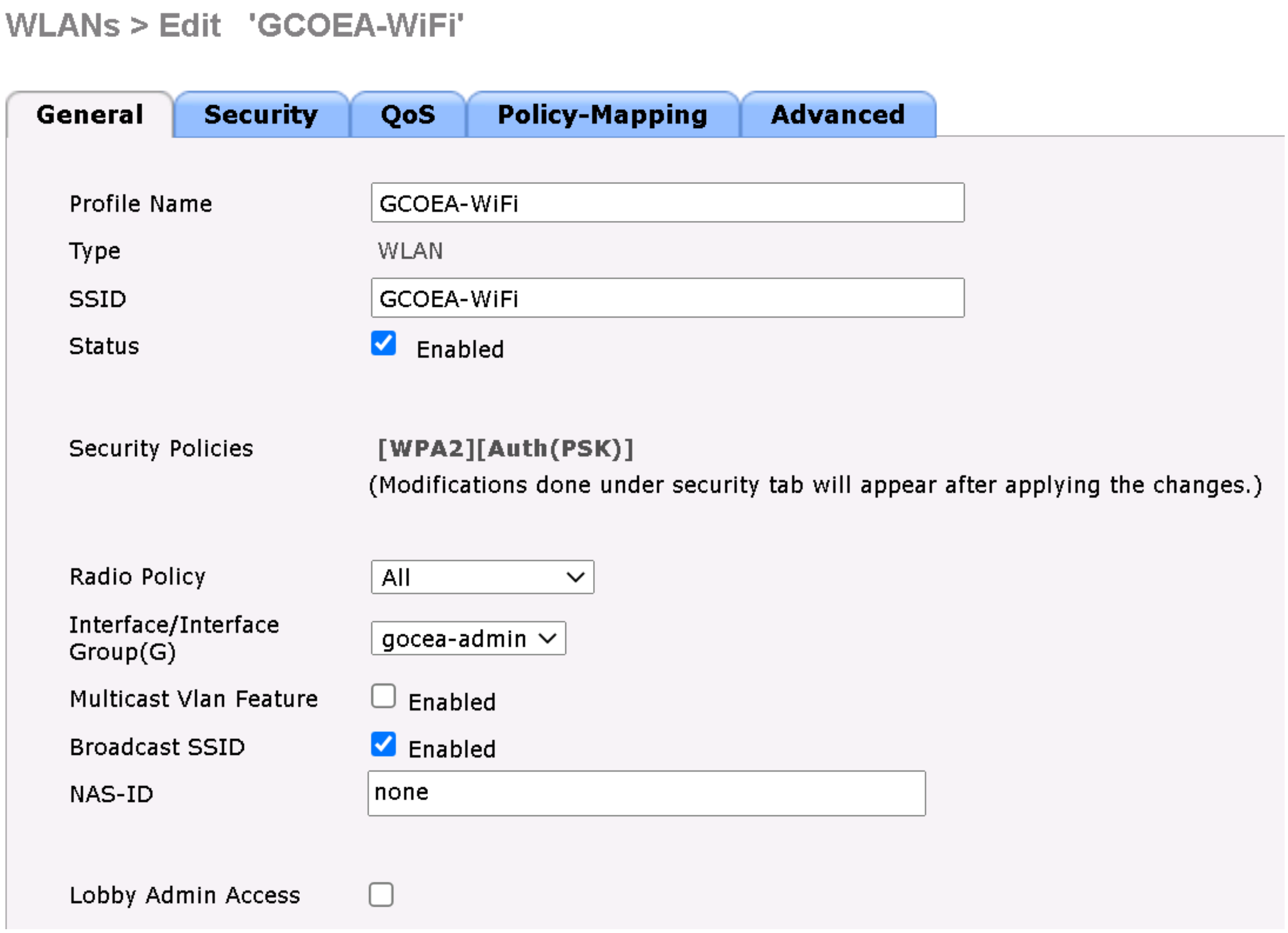
AP Name	IP Address(Ipv4/Ipv6)	AP Model
2_CIVIL_ENTRANCE	172.16.16.5	C9120AXI-D
B_ENTC_TERRANCE	172.16.16.18	AIR-AP1562E-D-K9
4_COMPUTER_ENGG	172.16.16.3	C9120AXI-D
1_ADMIN_ENTRANCE	172.16.16.16	C9120AXI-D
5_COMPUTER_ENGG	172.16.16.2	C9120AXI-D
B_IT_DEPT	172.16.16.10	AIR-AP1562E-D-K9
B_CIVIL_TERRACE	172.16.16.8	AIR-AP1562E-D-K9
6_IT_DEPT	172.16.16.11	C9120AXI-D
INDOOR-9120-AP	172.16.16.17	C9120AXI-D
3_IN_ENTC	172.16.16.6	C9120AXI-D
B_GIRLS_HOSTEL_1	172.16.16.36	AIR-AP1562E-D-K9
B_LIBRARY	172.16.16.12	AIR-AP1562E-D-K9
8_IN_GIRLSHOSTEL_NEW	172.16.16.35	C9120AXI-D
7_IN_LIBRARY	172.16.16.7	C9120AXI-D
8_GIRLS_HOSTEL_1	172.16.16.34	C9120AXI-D

Configuring Wlan SSID

Information about WLANs

This feature enables you to control up to WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. All controllers publish up to 16 WLANs to each connected access point. However, you can create till the maximum number of supported WLANs and then selectively publish these WLANs (using profiles and tags) to different access points for managing your wireless network in a better way.

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the controller to access.



WLANs > Edit 'GCOEA-WiFi'

Profile Name	GCOEA-WiFi
Type	WLAN
SSID	GCOEA-WiFi
Status	☑ Enabled
Security Policies	**[WPA2][Auth(PSK)]** (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	gocea-admin
Multicast Vlan Feature	☐ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none
Lobby Admin Access	☐

Monitoring wireless clients

Network Summary—Clients

This section displays the detailed information of clients that are associated with the access points in a list view.

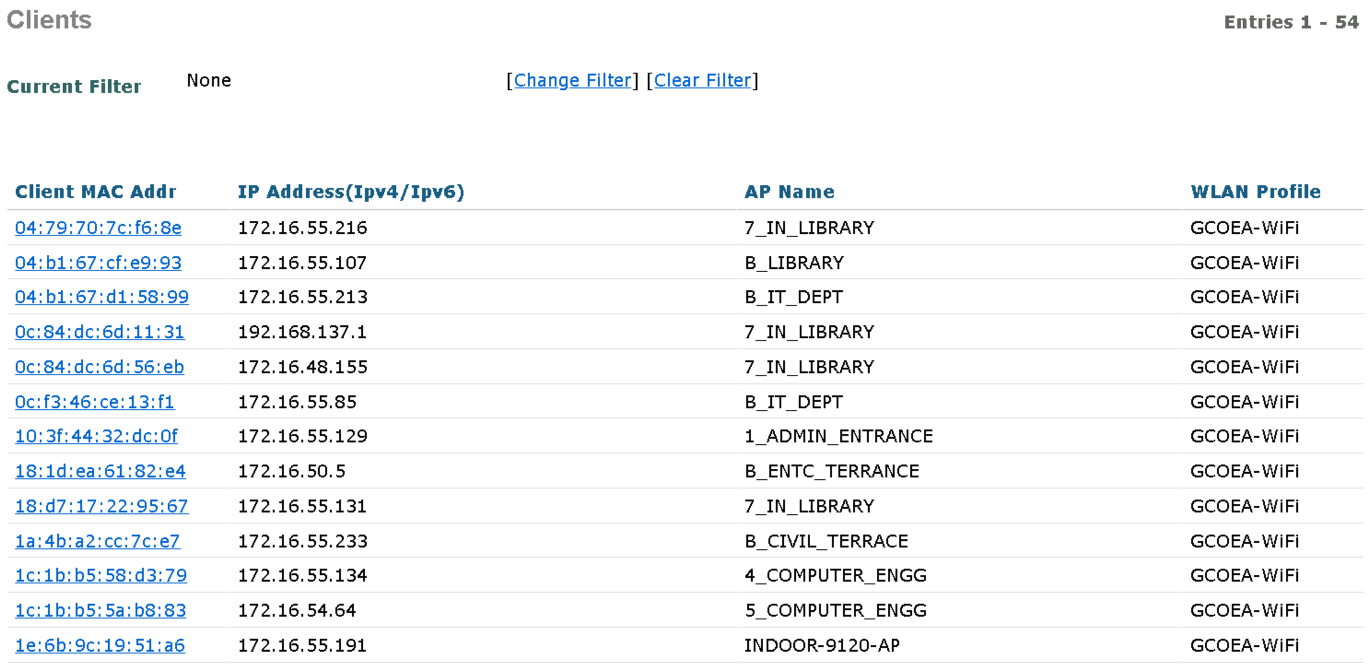
The **Client View** page is displayed when a client is selected. On this page, the client's general details are shown. Click **Connection Score** value to see the connection quality between the client and the AP.
There are two info graphic representations on the **Client View** page.

- The first infographic shows the connection stage of the client.
- The second infographic shows the connectivity roadmap between the controller and the client. It also shows the types of connection and the path that is used in the network from the controller to the client.

The **Network and QoS** and the **Security Policy** dashlets show the status of their respective parameters.

The **Client View** page also offers debugging tools to assess the connectivity from the client with the controller. Tools available are:

- Ping Test—helps to know the connectivity status and the latency between the two systems in a network.
- Connection—shows the connection logs for a client.
- Event Log—records the events and the option to save the logs on to a spreadsheet.
- Packet Capture—select from the various options to get precise information about the flow of packets to help resolve issues.



Clients

Entries 1 - 54

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile
04:79:70:7c:f6:8e	172.16.55.216	7_IN_LIBRARY	GCOEA-WiFi
04:b1:67:cf:e9:93	172.16.55.107	B_LIBRARY	GCOEA-WiFi
04:b1:67:d1:58:99	172.16.55.213	B_IT_DEPT	GCOEA-WiFi
0c:84:dc:6d:11:31	192.168.137.1	7_IN_LIBRARY	GCOEA-WiFi
0c:84:dc:6d:56:eb	172.16.48.155	7_IN_LIBRARY	GCOEA-WiFi
0c:f3:46:ce:13:f1	172.16.55.85	B_IT_DEPT	GCOEA-WiFi
10:3f:44:32:dc:0f	172.16.55.129	1_ADMIN_ENTRANCE	GCOEA-WiFi
18:1d:ea:61:82:e4	172.16.50.5	B_ENTC_TERRANCE	GCOEA-WiFi
18:d7:17:22:95:67	172.16.55.131	7_IN_LIBRARY	GCOEA-WiFi
1a:4b:a2:cc:7c:e7	172.16.55.233	B_CIVIL_TERRACE	GCOEA-WiFi
1c:1b:b5:58:d3:79	172.16.55.134	4_COMPUTER_ENGG	GCOEA-WiFi
1c:1b:b5:5a:b8:83	172.16.54.64	5_COMPUTER_ENGG	GCOEA-WiFi
1e:6b:9c:19:51:a6	172.16.55.191	INDOOR-9120-AP	GCOEA-WiFi

Cisco Firepower 2110 NGFW Appliance

Cisco Firepower 2100 Series appliances

The Cisco Firepower 2100 Series is a family of four threat-focused security platforms that deliver business resiliency and superior threat defense. They offers exceptional sustained performance when advanced threat functions are enabled. These platforms uniquely incorporate an innovative dual multicore CPU architecture that optimizes firewall, cryptographic, and threat inspection functions. The series' firewall throughput range addresses use cases from the Internet edge to the data center. Network Equipment Building Standards (NEBS)- compliance is supported by the Cisco Firepower 2130 platform. 2100 Series platforms run either the Cisco Secure Firewall ASA or Threat Defense (FMC) software. They can be deployed in both firewall and dedicated IPS modes.

Cisco Firepower 2100 series summary:

Model	Firewall	NGFW	IPS Throughput	Interfaces	Optional interfaces
FPR-2130	10G	5.4G	5.4G	12 x RJ45, 4 x SFP+	10G SFP+, 1/10G FTW

Cisco Firepower 2110 NGFW Appliance Deployment Includes:

- Configuring interfaces
- Configuring routing
- Configuring network objects
- Configuring network policies
- Deploying web access filter
- Access rule monitoring
- Smart license registration
- Backup & restore
- Firewall database updates
- ISP link redundancy

Configuring Interfaces

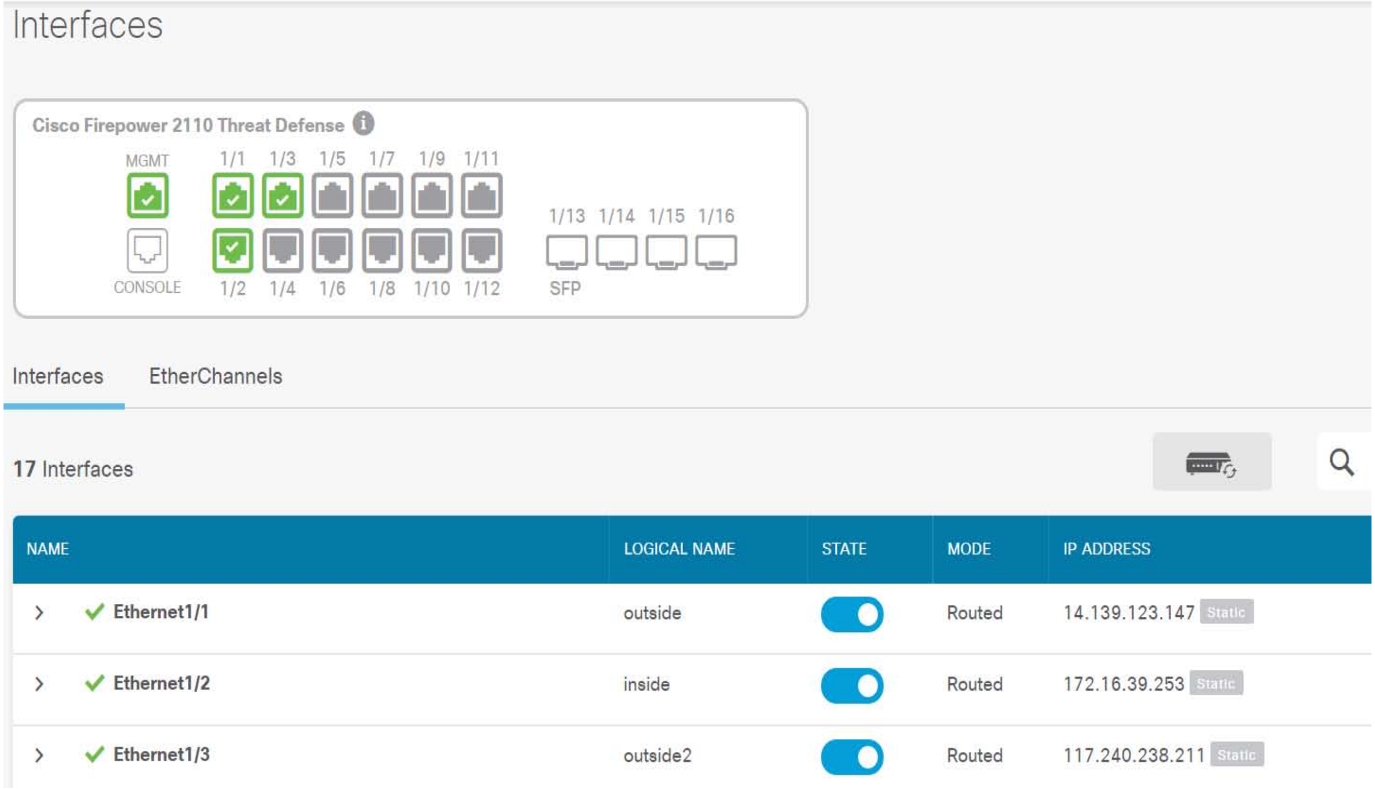
About FTD Interfaces

The FTD includes data interfaces as well as a management/diagnostic interface.

When you attach a cable to an interface connection (physically or virtually), you need to configure the interface. At minimum, you need to name the interface and enable it for it to pass traffic. If the interface is a member of a bridge group, this is sufficient. For non-bridge group members, you also need to give the interface an IP address. If you intend to create VLAN subinterfaces rather than a single physical interface on a given port, you would typically configure the IP addresses on the subinterface, not on the physical interface. VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs, which is useful when you connect to a trunk port on a switch. You do not configure IP addresses on passive interfaces.

We have configured a LAN interface that enables the GUI access of the appliance. Traffic from all departmental Vlans is routed to LAN interface. We have configured two WAN interfaces as we have two ISPs. The primary is NKN ISP link and the secondary is BSNL ISP link. Configured interface include inside and outside interfaces.

Refer image as below:



Interfaces

Cisco Firepower 2110 Threat Defense

17 Interfaces

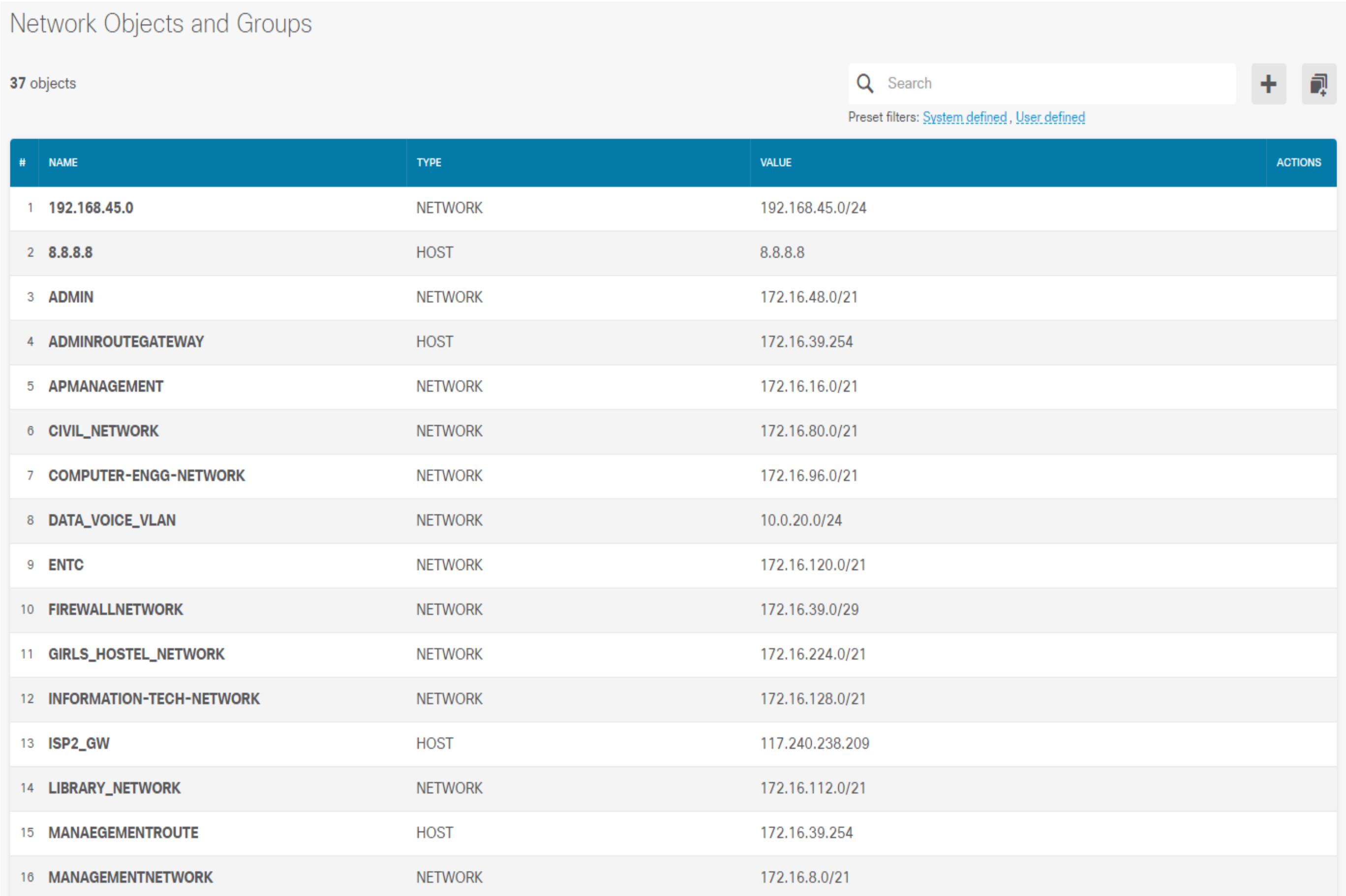
NAME	LOGICAL NAME	STATE	MODE	IP ADDRESS
› ✓ Ethernet1/1	outside	●	Routed	14.139.123.147 Static
› ✓ Ethernet1/2	inside	●	Routed	172.16.39.253 Static
› ✓ Ethernet1/3	outside2	●	Routed	117.240.238.211 Static

Configuring Network Objects:

Use network group and network objects (collectively referred to as network objects) to define the addresses of hosts or networks. You can then use the objects in security policies for purposes of defining traffic matching criteria, or in settings to define the addresses of servers or other resources.

A network object defines a single host or network address, whereas a network group object can define more than one address.

As we have configured separate Vlans for different departments in the campus likewise we have created network objects associated to configured Vlans in FPR for traffic matching criteria. Traffic from only configured objects are allowed in the network.



Network Objects and Groups

37 objects

#	NAME	TYPE	VALUE	ACTIONS
1	192.168.45.0	NETWORK	192.168.45.0/24	
2	8.8.8.8	HOST	8.8.8.8	
3	ADMIN	NETWORK	172.16.48.0/21	
4	ADMINROUTEGATEWAY	HOST	172.16.39.254	
5	APMANAGEMENT	NETWORK	172.16.16.0/21	
6	CIVIL_NETWORK	NETWORK	172.16.80.0/21	
7	COMPUTER-ENGG-NETWORK	NETWORK	172.16.96.0/21	
8	DATA_VOICE_VLAN	NETWORK	10.0.20.0/24	
9	ENTC	NETWORK	172.16.120.0/21	
10	FIREWALLNETWORK	NETWORK	172.16.39.0/29	
11	GIRLS_HOSTEL_NETWORK	NETWORK	172.16.224.0/21	
12	INFORMATION-TECH-NETWORK	NETWORK	172.16.128.0/21	
13	ISP2_GW	HOST	117.240.238.209	
14	LIBRARY_NETWORK	NETWORK	172.16.112.0/21	
15	MANAEGEMENTROUTE	HOST	172.16.39.254	
16	MANAGEMENTNETWORK	NETWORK	172.16.8.0/21	

Configuring Routing of Network Objects:

Configuring Static Routes

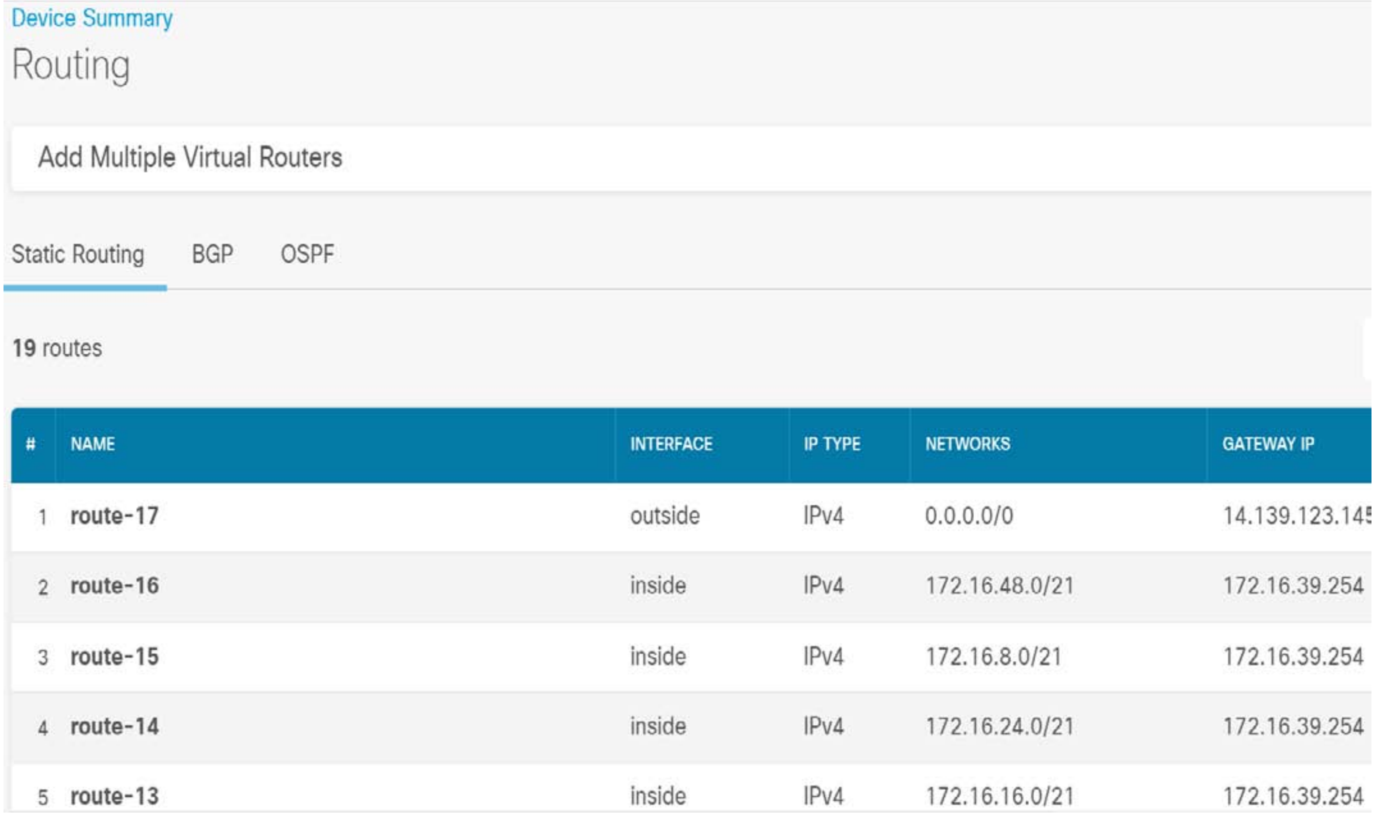
Define static routes to tell the system where to send packets that are not bound for networks that are directly connected to the interfaces on the system.

You need at least one static route, the default route, for network 0.0.0.0/0. This route defines where to send packets whose egress interface cannot be determined by existing NAT xlates (translations) or static NAT rules, or other static routes.

You might need other static routes if the default gateway cannot be used to get to all networks. For example, the default route is usually an upstream router on the outside interface. If there are additional inside networks that are not directly connected to the device, and they cannot be accessed through the default gateway, you need static routes for each of those inside networks.

You cannot define static routes for the networks that are directly connected to system interfaces. The system automatically creates these routes.

We have configured static routes for all network objects and the gateway is IP address of Firewall Vlan 172.16.39.254



Device Summary

Routing

19 routes

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP
1	route-17	outside	IPv4	0.0.0.0/0	14.139.123.145
2	route-16	inside	IPv4	172.16.48.0/21	172.16.39.254
3	route-15	inside	IPv4	172.16.8.0/21	172.16.39.254
4	route-14	inside	IPv4	172.16.24.0/21	172.16.39.254
5	route-13	inside	IPv4	172.16.16.0/21	172.16.39.254

Configuring Network security Policies:

Configuring the Access Control Policy

Use the access control policy to control access to network resources. The policy consists of a set of ordered rules, which are evaluated from top to bottom. The rule applied to traffic is the first one where all the traffic criteria are matched. If no rules match the traffic, the default action shown at the bottom of the page is applied.

To configure the access control policy, select **Policies** > **Access Control**.

The access control table lists all rules in order. For each rule:

- Click the **>** button next to the rule number in the left-most column to open the rule diagram. The diagram can help you visualize how the rule controls traffic. Click the button again to close the diagram.
- Most cells allow inline editing. For example, you can click the action to select a different one, or click a source network object to add or change the source criteria.
- To move a rule, hover over the rule until you get the move icon ( ), then click, drag, and drop the rule to the new location. You can also move a rule by editing it and selecting the new location in the **Order** list. It is critical that you put the rules in the order that you want them processed. Specific rules should be near the top, especially for rules that define exceptions to more general rules
- The right-most column contains the action buttons for a rule; mouse over the cell to see the buttons.
- Click the **Toggle H it C ounts** above the table to add or remove the Hit Counts column in the table. The Hit Count column appears to the right of the Name column with the total hit count for the rule and the date and time of the last hit. The hit count information is fetched at the time you click the toggle button. Click the **refresh** icon to get the latest information.
- If any rules have problems, for example, because of removed or changed URL categories, click the **See P roblem R ules** link next to the search box to filter the table to show only those rules. Please edit and correct (or delete) these rules, so that they will provide the service that you require.

Configuring Access Control Rules

Use access control rules to control access to network resources. Rules in the access control policy are evaluated from top to bottom. The rule applied to traffic is the first one where all the traffic criteria are matched.

Procedure

Step 1 Select **Policies** > **Access Control**.

Step 2 Do any of the following:

- To create a new rule, click the **+** button.
- To edit an existing rule, click the edit icon for the rule.

To delete a rule you no longer need, click the delete icon for the rule.

Step 3 In **Order**, select where you want to insert the rule in the ordered list of rules.

Rules are applied on a first-match basis, so you must ensure that rules with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

The default is to add the rule to the end of the list. If you want to change a rule's location later, edit this option.

Step 4 In **Title**, enter a name for the rule.

The name cannot contain spaces. You can use alphanumeric characters and these special characters: + . _ -

Step 5 Select the action to apply to matching traffic.

- **Trust**—Allow traffic without further inspection of any kind.
- **Allow**—Allow the traffic subject to the intrusion and other inspection settings in the policy.
- **Block**—Drop the traffic unconditionally. The traffic is not inspected.

Step 6 Define the traffic matching criteria using any combination of the following tabs:

- **Source/Destination**—The security zones (interfaces) through which the traffic passes, the IP addresses or the country or continent (geographical location) for the IP address, or the protocols and ports used in the traffic. The default is any zone, address, geographical location, protocol, and port. See Source/Destination Criteria.
- **Application**—The application, or a filter that defines applications by type, category, tag, risk, or business relevance. The default is any application. See Application Criteria.
- **URL**—The URL or URL category of a web request. The default is any URL. See URL Criteria.
- **Users**—The identity source, user or user group. Your identity policies determine whether user and group information is available for traffic matching. You must configure identity policies to use this criteria. See User Criteria.

To modify a condition, you click the **+** button within that condition, select the desired object or element, and click **OK** in the popup dialog box. If the criterion requires an object, you can click **Create New *Object*** if the object you require does not exist. Click the **x** for an object or element to remove it from the policy.

When adding conditions to access control rules, consider the following tips:

- You can configure multiple conditions per rule. Traffic must match all the conditions in the rule for the rule to apply to traffic. For example, you can use a single rule to perform URL filtering for specific hosts or networks.
- For each condition in a rule, you can add up to 50 criteria. Traffic that matches any of a condition's criteria satisfies the condition. For example, you can use a single rule to apply application control for up to 50 applications or application filters. Thus, there is an OR relationship among the items in a single condition, but an AND relationship between condition types (for example, between source/destination and application).
- Some features require that you enable the appropriate license.

Step 7 (Optional.) For policies that use the Allow action, you can configure further inspection on unencrypted traffic. Click one of the following links:

- **Intrusion Policy**—Select **Intrusion Policy** > **On** and select the intrusion inspection policy to inspect traffic for intrusions and exploits. See Intrusion Policy Settings.
- **File Policy**—Select the file policy to inspect traffic for files that contain malware and for files that should be blocked. See File Policy Settings.

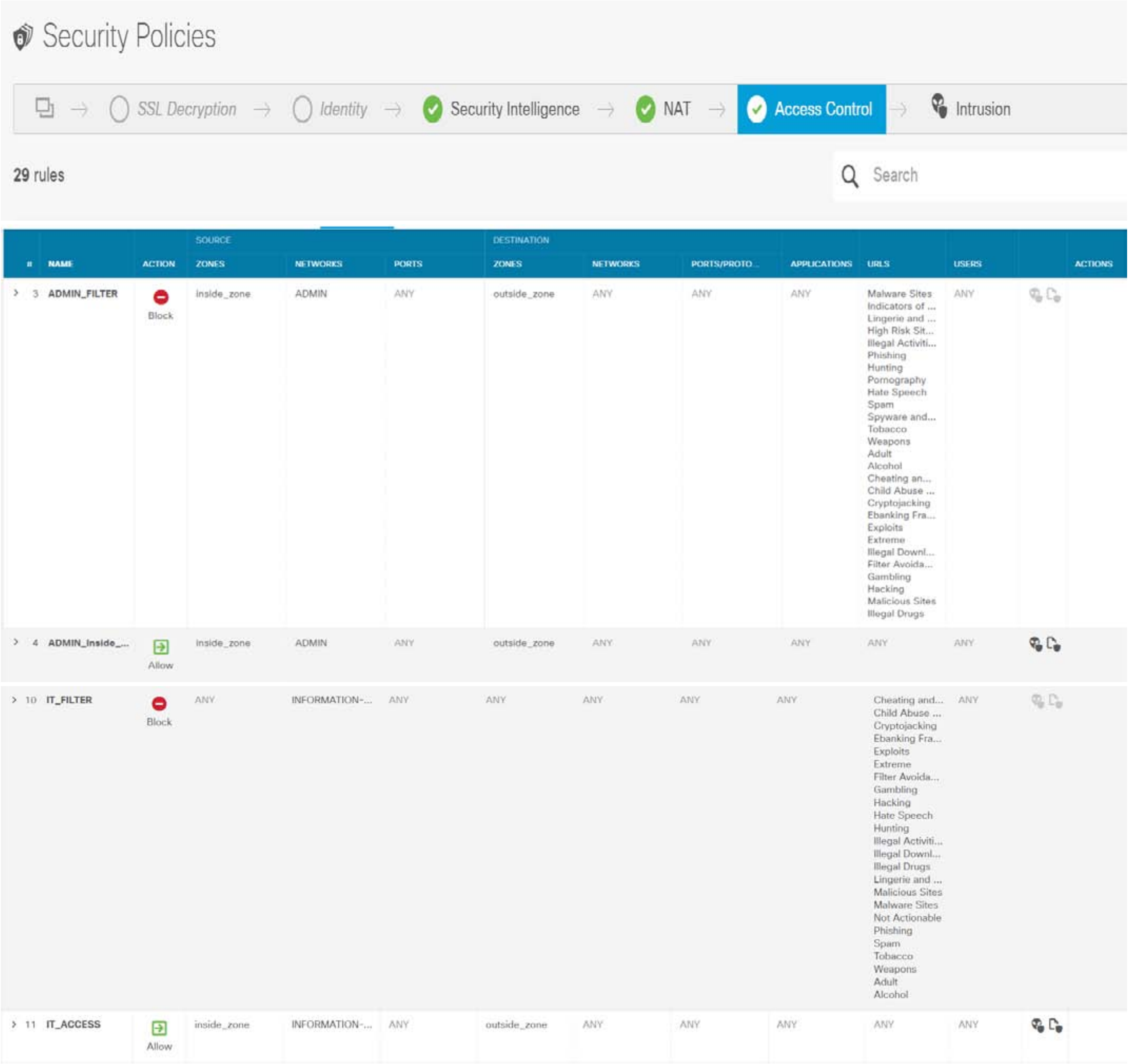
Step 8 (Optional.) Configure logging for the rule.

By default, connection events are not generated for traffic that matches a rule, although file events are generated by default if you select a file policy. You can change this behavior. You must enable logging for traffic that matches the policy to be included in dashboard data or Event Viewer. See Logging Settings.

Intrusion events are always generated for intrusion rules set to drop or alert regardless of the logging configuration on the matching access rule.

Step 9 Click **OK**.

We have configured secure access control policies that allow the user traffic for all objects created that represents Vlans of different departments in the campus.
Refer access control policy for Admin and IT department as below:



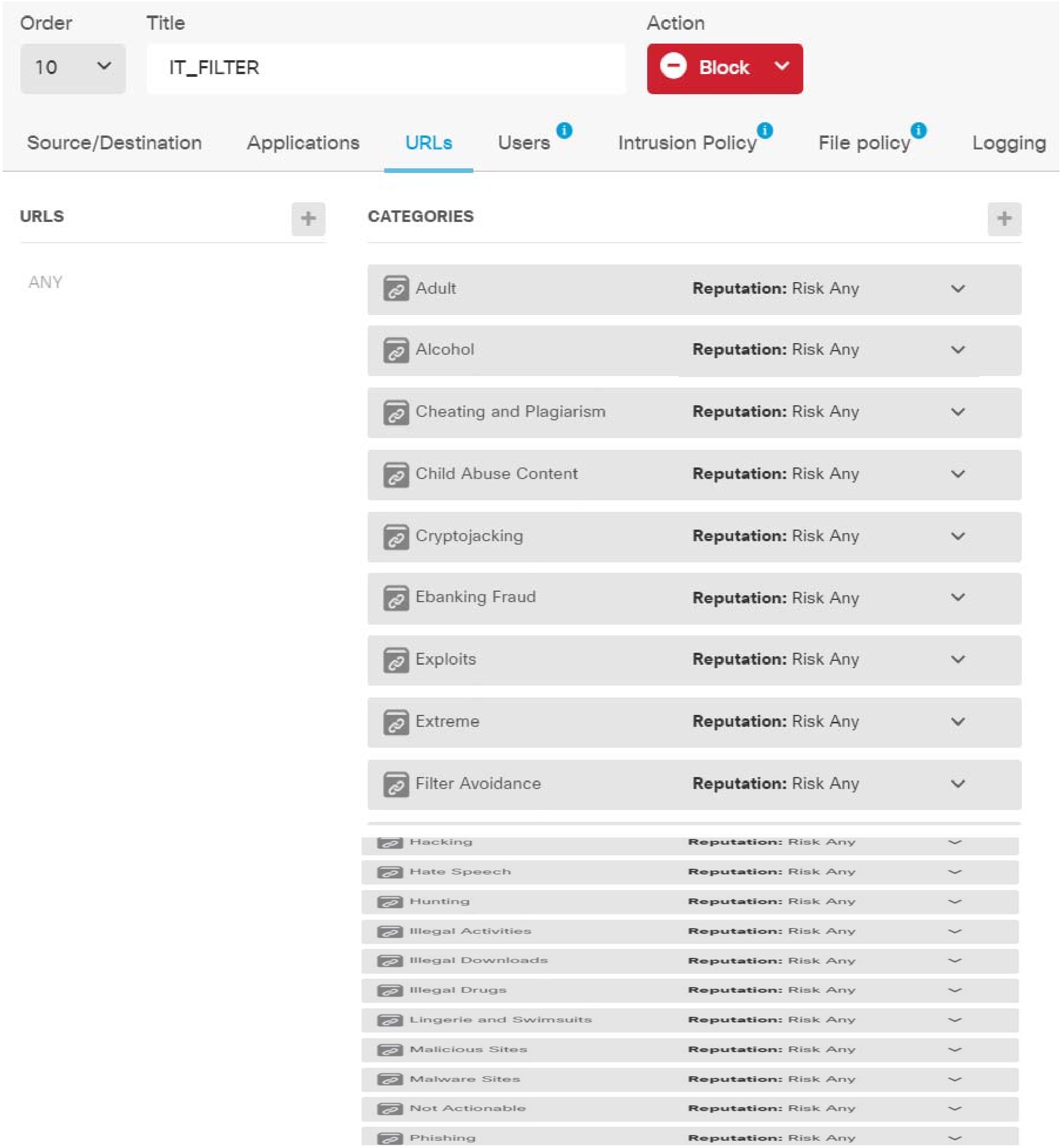
Security Policies
SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion
Search

29 rules

			SOURCE			DESTINATION							
#	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO...	APPLICATIONS	URLS	USERS		ACTIONS
3	ADMIN_FILTER	Block	inside_zone	ADMIN	ANY	outside_zone	ANY	ANY	ANY	Malware Sites Indicators of ... Lingerie and ... High Risk Sit... Illegal Activiti... Phishing Hunting Pornography Hate Speech Spam Spyware and... Tobacco Weapons Adult Alcohol Cheating an... Child Abuse ... Cryptojacking Ebanking Fra... Exploits Extreme Illegal Downl... Filter Avoida... Gambling Hacking Malicious Sites Illegal Drugs	ANY		
4	ADMIN_Inside_...	Allow	inside_zone	ADMIN	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY		
10	IT_FILTER	Block	ANY	INFORMATION-...	ANY	ANY	ANY	ANY	ANY	Cheating and... Child Abuse ... Cryptojacking Ebanking Fra... Exploits Extreme Filter Avoida... Gambling Hacking Hate Speech Hunting Illegal Activiti... Illegal Downl... Illegal Drugs Lingerie and ... Malicious Sites Malware Sites Not Actionable Phishing Spam Tobacco Weapons Adult Alcohol	ANY		
11	IT_ACCESS	Allow	inside_zone	INFORMATION-...	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY		

Deploying security web access filter

Web access filter is created to block browsing of non-relevant websites in the network. Numerous of websites categories that can infect the network will malwares etc are blocked. Refer the categories blocked as below:



Order: 10
Title: IT_FILTER
Action: Block

URLS: ANY

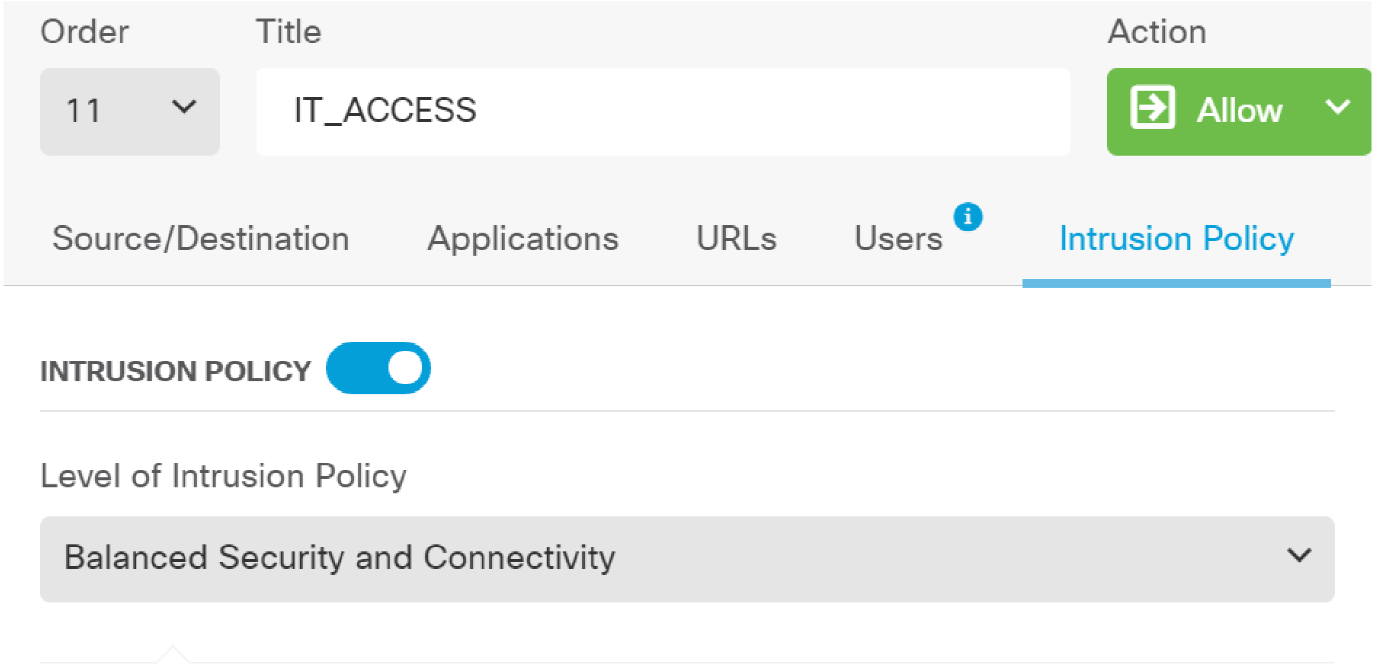
CATEGORIES	
Adult	**Reputation:** Risk Any
Alcohol	**Reputation:** Risk Any
Cheating and Plagiarism	**Reputation:** Risk Any
Child Abuse Content	**Reputation:** Risk Any
Cryptojacking	**Reputation:** Risk Any
Ebanking Fraud	**Reputation:** Risk Any
Exploits	**Reputation:** Risk Any
Extreme	**Reputation:** Risk Any
Filter Avoidance	**Reputation:** Risk Any
Hacking	**Reputation:** Risk Any
Hate Speech	**Reputation:** Risk Any
Hunting	**Reputation:** Risk Any
Illegal Activities	**Reputation:** Risk Any
Illegal Downloads	**Reputation:** Risk Any
Illegal Drugs	**Reputation:** Risk Any
Lingerie and Swimsuits	**Reputation:** Risk Any
Malicious Sites	**Reputation:** Risk Any
Malware Sites	**Reputation:** Risk Any
Not Actionable	**Reputation:** Risk Any
Phishing	**Reputation:** Risk Any

Configuring Intrusion policy in allow access control rule:

Intrusion policy is enabled in allow access control rule. Intrusion policies as a last line of defense against unwanted traffic that you are otherwise allowing. An intrusion policy examines decoded packets for intrusions, exploits, and other attacks based on patterns, and can block or alter malicious traffic. Cisco delivers several intrusion policies with the Firepower system. These policies are designed by the Cisco Talos Security Intelligence and Research Group, who set the intrusion and preprocessor rule states and advanced settings. We have selected Balanced Security and Connectivity intrusion policy for all access control rules.

Balanced Security and Connectivity

This policy is designed to balance overall network performance with network infrastructure security. This policy is appropriate for most networks. Select this policy for most situations where you want to apply intrusion prevention.



Order: 11
Title: IT_ACCESS
Action: Allow

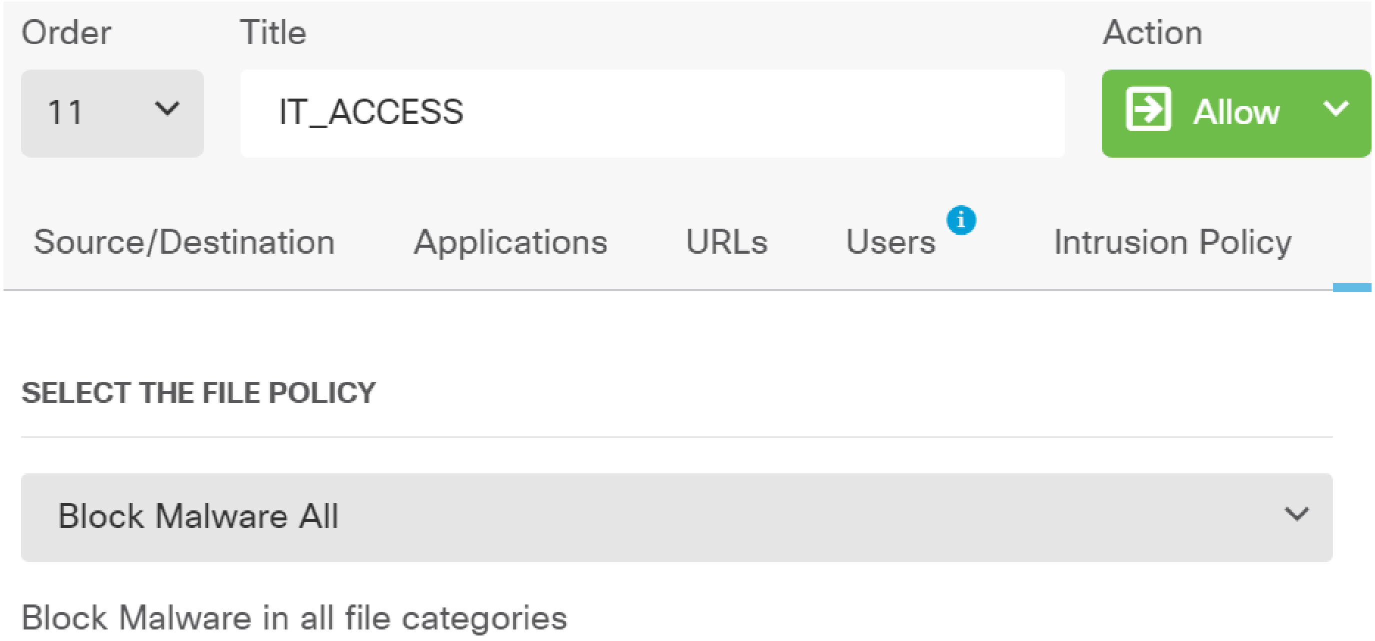
INTRUSION POLICY: on

Level of Intrusion Policy: Balanced Security and Connectivity

Configuring file policy in allow access control rules:

CONTROLLING FILES AND MALWARE

Use file policies to detect and prevent malicious software, or malware You can also use file policies to perform file control, which allows control over all files of a specific type regardless of whether the files contain malware.



Order: 11

Title: IT_ACCESS

Action: Allow

SELECT THE FILE POLICY

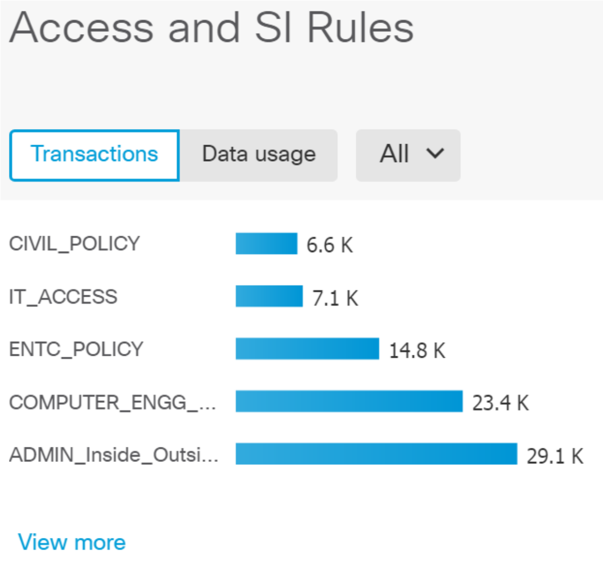
Block Malware All

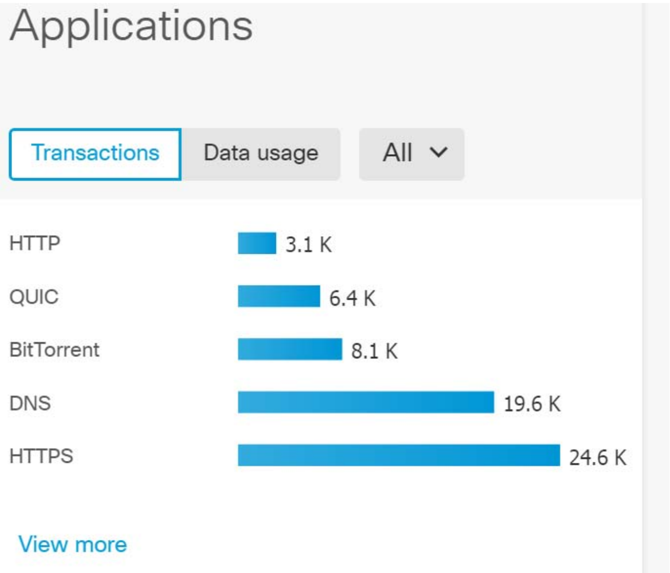
Block Malware in all file categories

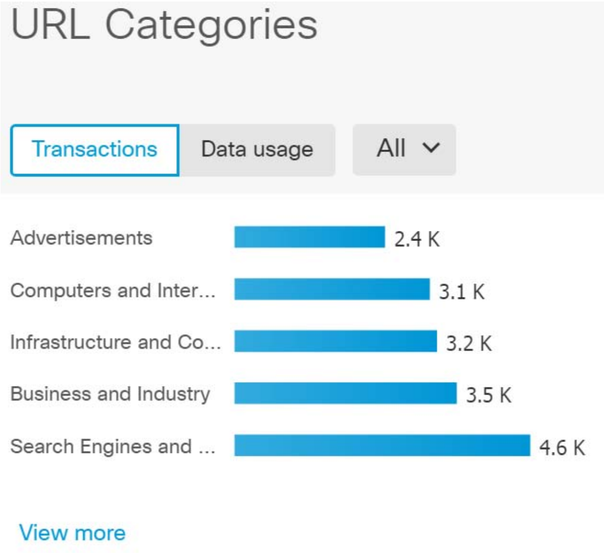
Access rule monitoring:

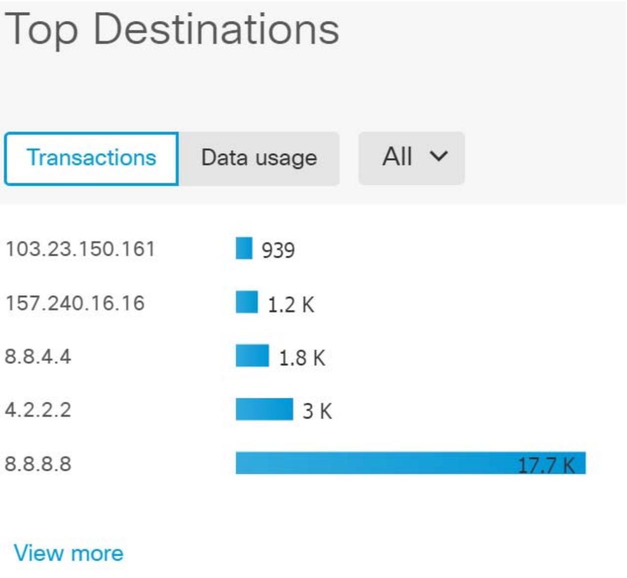
Monitoring Traffic and System Dashboards

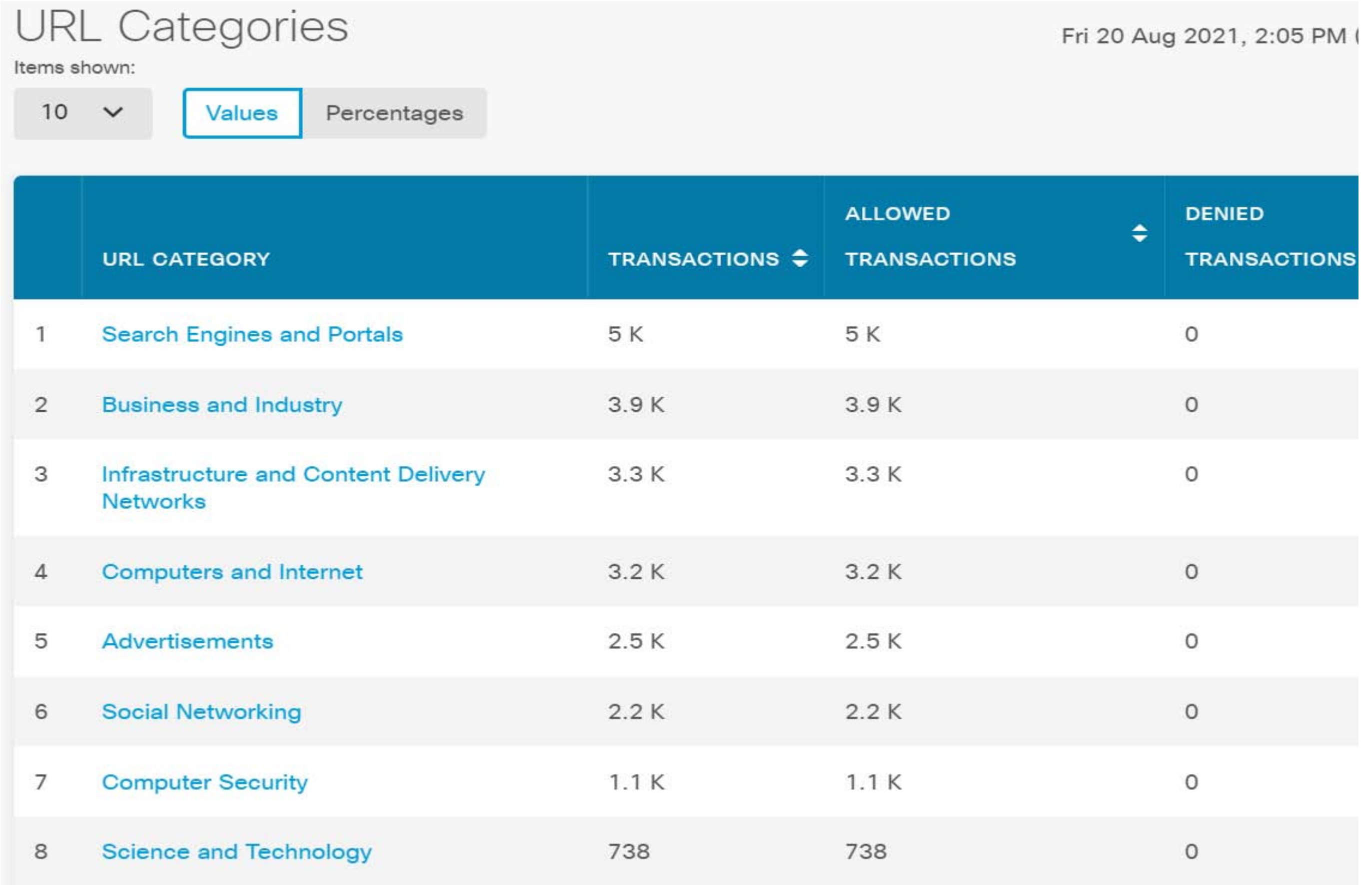
The system includes several dashboards that you can use to analyze the traffic going through the device and the results of your security policy. Use the information to evaluate the overall efficacy of your configuration and to identify and resolve network problems.






URL Categories
Transactions
Data usage
All
Advertisements 2.4 K
Computers and Inter... 3.1 K
Infrastructure and Co... 3.2 K
Business and Industry 3.5 K
Search Engines and ... 4.6 K
View more



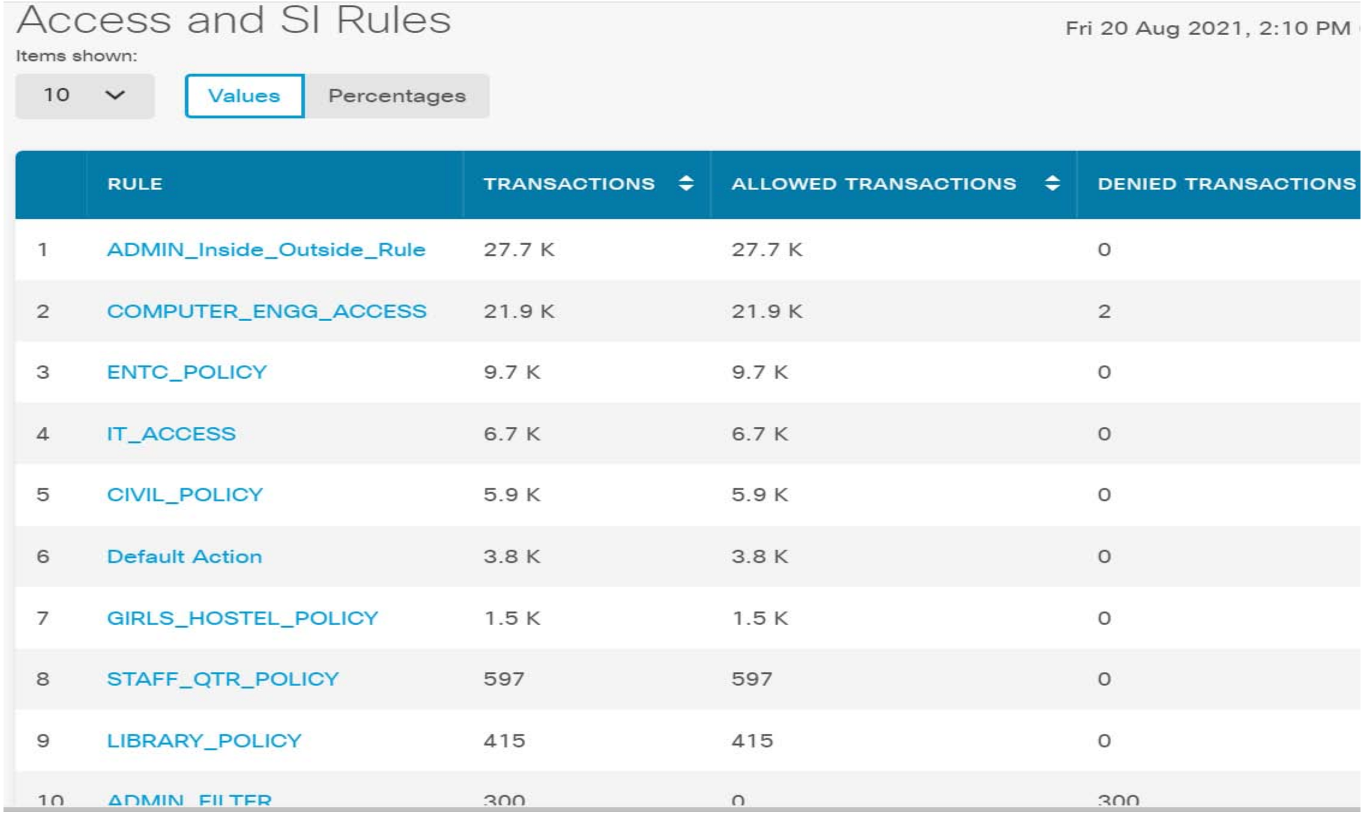


URL Categories

Fri 20 Aug 2021, 2:05 PM (

Items shown: 10

	URL CATEGORY	TRANSACTIONS	ALLOWED TRANSACTIONS	DENIED TRANSACTIONS
1	Search Engines and Portals	5 K	5 K	0
2	Business and Industry	3.9 K	3.9 K	0
3	Infrastructure and Content Delivery Networks	3.3 K	3.3 K	0
4	Computers and Internet	3.2 K	3.2 K	0
5	Advertisements	2.5 K	2.5 K	0
6	Social Networking	2.2 K	2.2 K	0
7	Computer Security	1.1 K	1.1 K	0
8	Science and Technology	738	738	0



Access and SI Rules

Fri 20 Aug 2021, 2:10 PM

Items shown: 10

	RULE	TRANSACTIONS	ALLOWED TRANSACTIONS	DENIED TRANSACTIONS
1	ADMIN_Inside_Outside_Rule	27.7 K	27.7 K	0
2	COMPUTER_ENGG_ACCESS	21.9 K	21.9 K	2
3	ENTC_POLICY	9.7 K	9.7 K	0
4	IT_ACCESS	6.7 K	6.7 K	0
5	CIVIL_POLICY	5.9 K	5.9 K	0
6	Default Action	3.8 K	3.8 K	0
7	GIRLS_HOSTEL_POLICY	1.5 K	1.5 K	0
8	STAFF_QTR_POLICY	597	597	0
9	LIBRARY_POLICY	415	415	0
10	ADMIN_FILTER	300	0	300

Smart license registration:

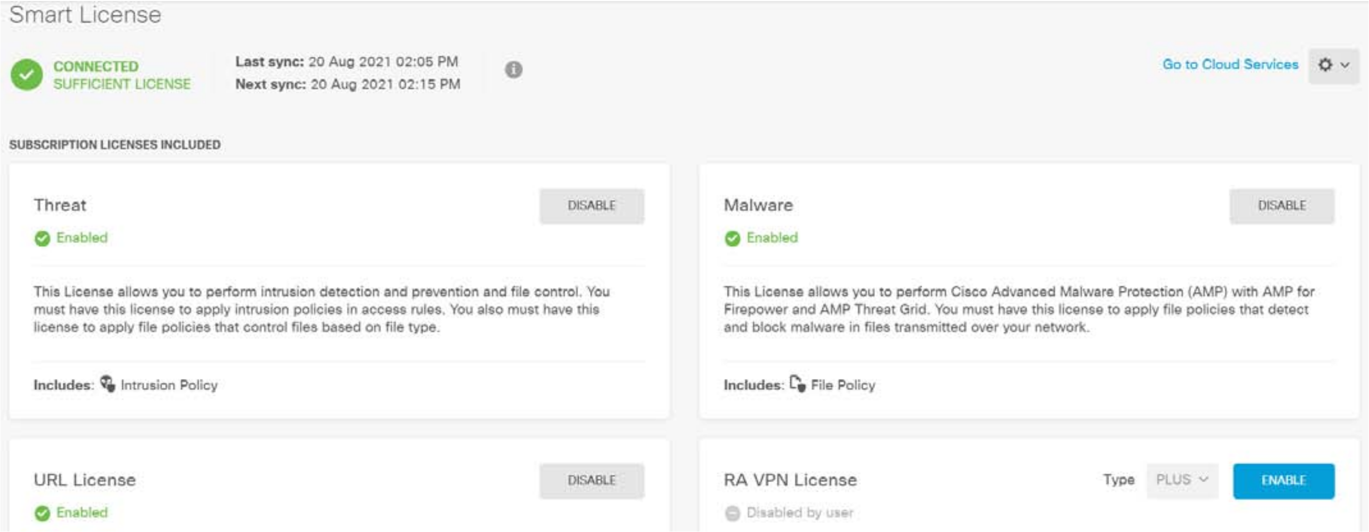
Managing Smart Licenses

Use the Smart License page to view the current license status for the system. The system must be licensed.

The page shows you whether you are using the 90-day evaluation license, or if you have registered with the Cisco Smart Software Manager. Once registered, you can see the status of the connection to the Cisco Smart Software Manager as well as the status for each type of license.

Usage Authorization identifies the Smart License Agent status:

- Authorized (“Connected,” “Sufficient Licenses”)—The device has contacted and registered successfully with the License Authority, which has authorized the license entitlements for the appliance. The device is now In-Compliance.
- Out-of-Compliance—There is no available license entitlement for the device. Licensed features continue to work. However, you must either purchase or free up additional entitlements to become In-Compliance.
- Authorization Expired—The device has not communicated with the Licensing Authority in 90 or more days. Licensed features continue to work. In this state, the Smart License Agent retries its authorization requests. If a retry succeeds, the agent enters either an Out-of-Compliance or Authorized state, and begins a new Authorization Period. Try manually synchronizing the device.



Smart License

CONNECTED
SUFFICIENT LICENSE

Last sync: 20 Aug 2021 02:05 PM
Next sync: 20 Aug 2021 02:15 PM

SUBSCRIPTION LICENSES INCLUDED

Threat
Enabled

This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

Malware
Enabled

This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.

Includes: File Policy

URL License
Enabled

RA VPN License
Type: PLUS
Disabled by user

Firewall database updates:

Overview of System Database and Feed Updates

Firepower Threat Defense uses the following databases and feeds to provide advanced services.

Intrusion rules

As new vulnerabilities become known, the Cisco Talos Intelligence Group (Talos) releases intrusion rule updates that you can import. These updates affect intrusion rules, preprocessor rules, and the policies that use the rules.

Intrusion rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates may also delete rules, provide new rule categories and default variables, and modify default variable values.

For changes made by an intrusion rule update to take effect, you must redeploy the configuration.

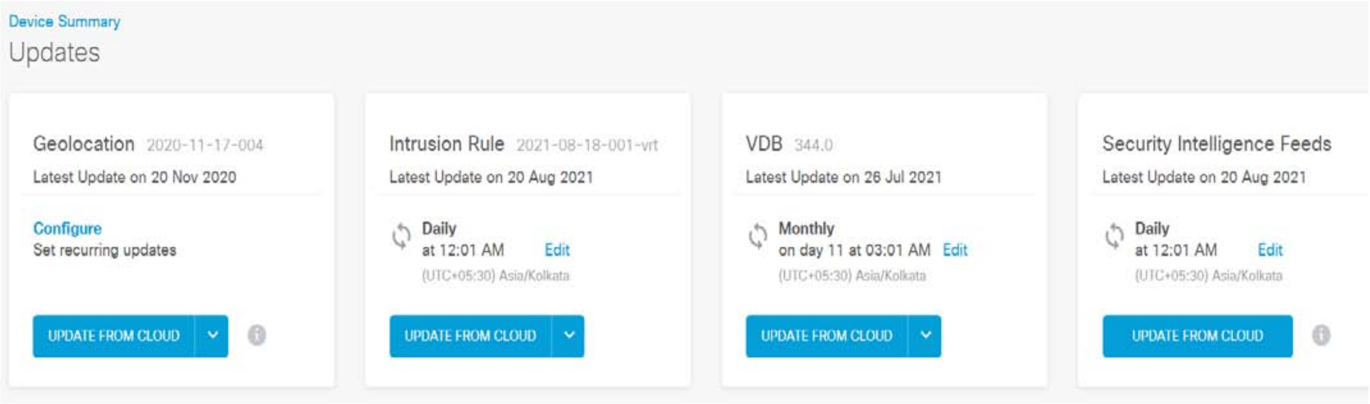
Intrusion rule updates may be large, so import rules during periods of low network use. On slow networks, an update attempt might fail, and you will need to retry.

Cisco Talos Intelligence Group (Talos) Security Intelligence Feeds

Talos provides access to regularly updated intelligence feeds for use in Security Intelligence policies. Sites representing security threats such as malware, spam, botnets, and phishing appear and disappear faster than you can update and deploy custom configurations. These feeds contain addresses and URLs for known threats. When the system updates a feed, you do not have to redeploy. The new lists are used for evaluating subsequent connections.

URL Category/Reputation Database

The system obtains the URL category and reputation database from Cisco Collective Security Intelligence (CSI). If you configure URL filtering access control rules that filter on category and reputation, requested URLs are matched against the database. You can configure database updates and some other URL filtering preferences on **System Settings** > **URL Filtering Pr eferences**. You cannot manage URL category/reputation database updates the same way you manage updates for the other system databases.



Device Summary
Updates

Geolocation 2020-11-17-004
Latest Update on 20 Nov 2020
Configure
Set recurring updates

Intrusion Rule 2021-08-18-001-vrt
Latest Update on 20 Aug 2021
Daily
at 12:01 AM Edit
(UTC+05:30) Asia/Kolkata

VDB 344.0
Latest Update on 26 Jul 2021
Monthly
on day 11 at 03:01 AM Edit
(UTC+05:30) Asia/Kolkata

Security Intelligence Feeds
Latest Update on 20 Aug 2021
Daily
at 12:01 AM Edit
(UTC+05:30) Asia/Kolkata

Cisco Prime Infrastructure

Version: 3.9

View Installed Updates

One Management and One Assurance of Enterprise Networks across wired and wireless / for One Network

Overview

Cisco Prime Infrastructure is a network management tool that supports lifecycle management of your entire network infrastructure from a single graphical interface. Cisco Prime Infrastructure provides network administrators a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust graphical interfaces make device deployments and operations simple and cost-effective.

To overcome these challenges, IT professionals need a comprehensive solution to manage, visualize, and monitor the network from a single graphical interface. Cisco Prime™ Infrastructure provides lifecycle management, assurance visibility, and troubleshooting capabilities network-wide - from the wireless user in the branch office, across the WAN. In essence, it is One Management and One Assurance, for One Network

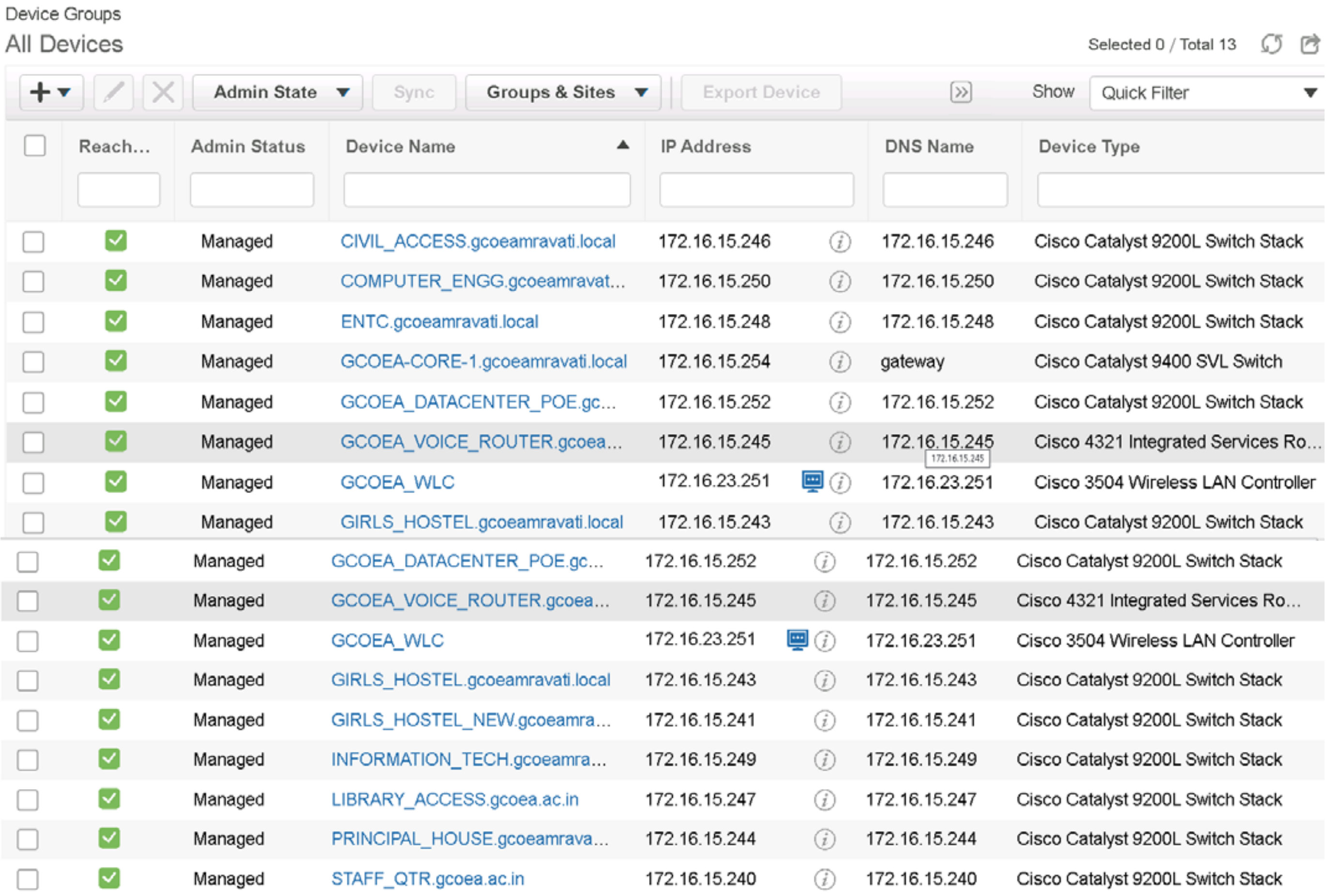
Cisco Prime Infrastructure highlights

Cisco Prime Infrastructure allows/helps you to manage your network more efficiently and effectively, thereby enabling you to achieve the highest levels of wireless and wired network performance, service assurance, and application-centric end-user experience.

- Single-pane-of-glass management
- Simplified deployment of Cisco® capabilities
- Deep Application Visibility
- Comprehensive coverage of enterprise mobility
- Unified assurance across network and compute
- Centralized visibility of distributed networks

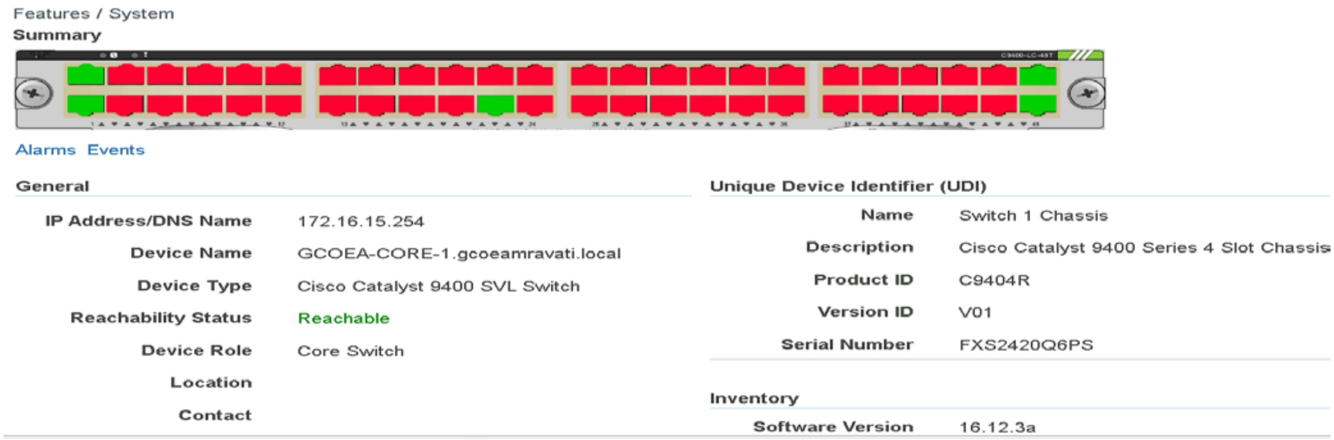
Creating Network Device Inventory:

To allow Prime to manage the wired and wireless network it is necessary to add all network devices in the campus. The network device and Prime communication is done using snmp. We have configured snmpv3 and 2. All the network devices are added in Prime as below:



☐	Reach...	Admin Status	Device Name ▲	IP Address		DNS Name	Device Type
☐	☑	Managed	CIVIL_ACCESS.gcoeamravati.local	172.16.15.246	ⓘ	172.16.15.246	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	COMPUTER_ENGG.gcoeamravat...	172.16.15.250	ⓘ	172.16.15.250	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	ENTC.gcoeamravati.local	172.16.15.248	ⓘ	172.16.15.248	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	GCOEA-CORE-1.gcoeamravati.local	172.16.15.254	ⓘ	gateway	Cisco Catalyst 9400 SVL Switch
☐	☑	Managed	GCOEA_DATACENTER_POE.gc...	172.16.15.252	ⓘ	172.16.15.252	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	GCOEA_VOICE_ROUTER.gcoea...	172.16.15.245	ⓘ	172.16.15.245	Cisco 4321 Integrated Services Ro...
☐	☑	Managed	GCOEA_WLC	172.16.23.251	🖥 ⓘ	172.16.23.251	Cisco 3504 Wireless LAN Controller
☐	☑	Managed	GIRLS_HOSTEL.gcoeamravati.local	172.16.15.243	ⓘ	172.16.15.243	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	GCOEA_DATACENTER_POE.gc...	172.16.15.252	ⓘ	172.16.15.252	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	GCOEA_VOICE_ROUTER.gcoea...	172.16.15.245	ⓘ	172.16.15.245	Cisco 4321 Integrated Services Ro...
☐	☑	Managed	GCOEA_WLC	172.16.23.251	🖥 ⓘ	172.16.23.251	Cisco 3504 Wireless LAN Controller
☐	☑	Managed	GIRLS_HOSTEL.gcoeamravati.local	172.16.15.243	ⓘ	172.16.15.243	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	GIRLS_HOSTEL_NEW.gcoeamra...	172.16.15.241	ⓘ	172.16.15.241	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	INFORMATION_TECH.gcoeamra...	172.16.15.249	ⓘ	172.16.15.249	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	LIBRARY_ACCESS.gcoea.ac.in	172.16.15.247	ⓘ	172.16.15.247	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	PRINCIPAL_HOUSE.gcoeamrava...	172.16.15.244	ⓘ	172.16.15.244	Cisco Catalyst 9200L Switch Stack
☐	☑	Managed	STAFF_QTR.gcoea.ac.in	172.16.15.240	ⓘ	172.16.15.240	Cisco Catalyst 9200L Switch Stack

On addition of network switches in Prime we can manage them through Prime and have a complete view of the cdp devices attached to the network switch and can monitor their performance.



General

IP Address/DNS Name	172.16.15.254
Device Name	GCOEA-CORE-1.gcoeamravati.local
Device Type	Cisco Catalyst 9400 SVL Switch
Reachability Status	Reachable
Device Role	Core Switch
Location	
Contact	

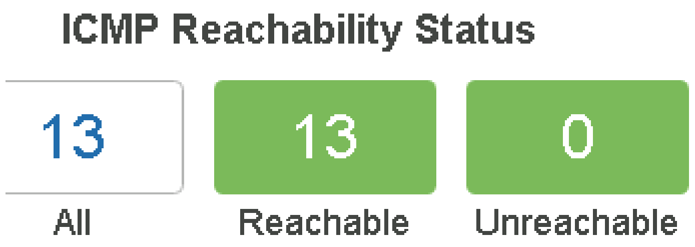
Unique Device Identifier (UDI)

Name	Switch 1 Chassis
Description	Cisco Catalyst 9400 Series 4 Slot Chassis
Product ID	C9404R
Version ID	V01
Serial Number	FXS2420Q6PS

Inventory

Software Version	16.12.3a

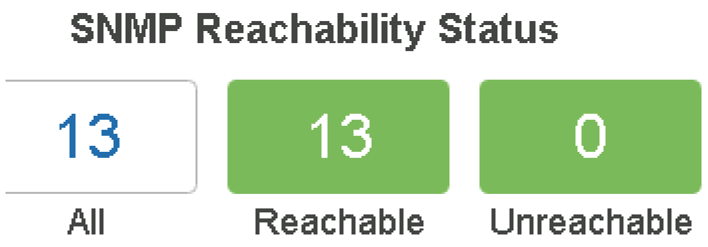
Monitoring:



ICMP Reachability Status

13	13	0
All	Reachable	Unreachable

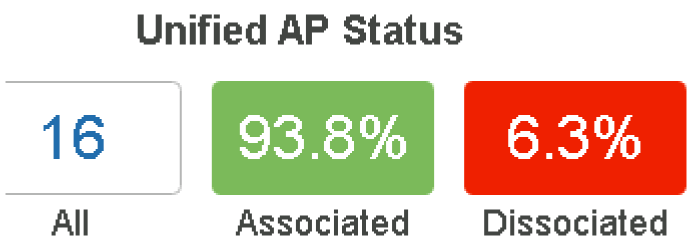
In real time Prime indicates ICMP reachability. It detects device ICMP lost and triggered alarm so that corrective action can be taken.



SNMP Reachability Status

13	13	0
All	Reachable	Unreachable

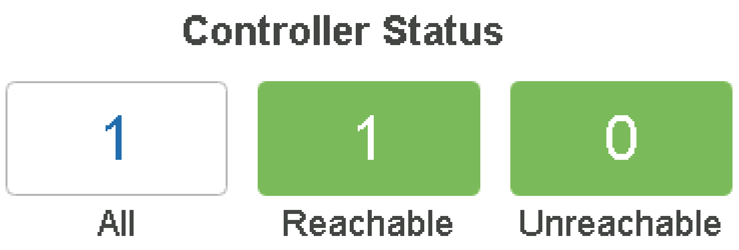
SNMP is used for communication between network devices and Prime. Prime displays the SNMP reachability status in real time.



Unified AP Status

16	93.8%	6.3%
All	Associated	Dissociated

Unified AP are discovered in Prime as we have added the wireless controller in Prime. The real time discovery status is shown in Prime as above.



Controller Status

1	1	0
All	Reachable	Unreachable

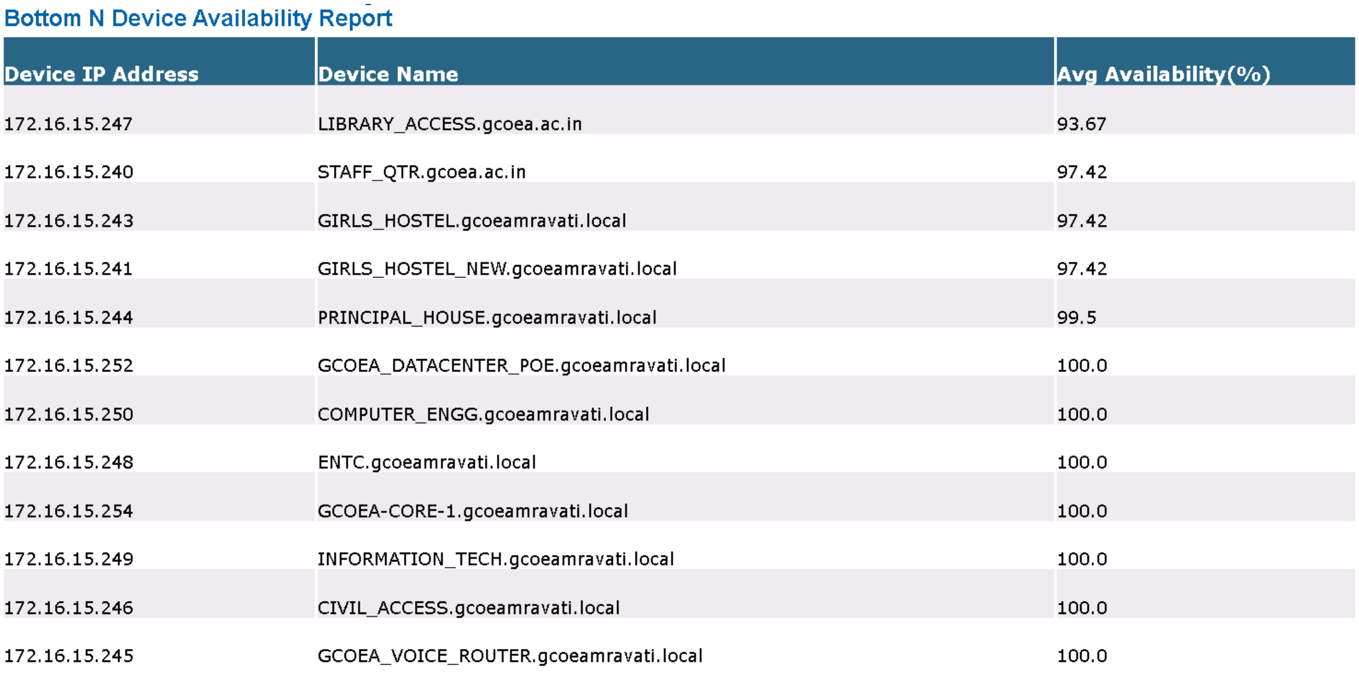
We can also monitor the wireless controller status in Prime as above.

Prime report launch pad:

Reports Overview

Reports provide information about system and network health as well as fault information. You can customize and schedule reports to run on a regular basis. Reports can present data in a tabular, or graphical format (or a mixture of these formats). You can also save reports in CSV or PDF format. The CSV or PDF files can be saved on the server for later download, or sent to an e-mail address.

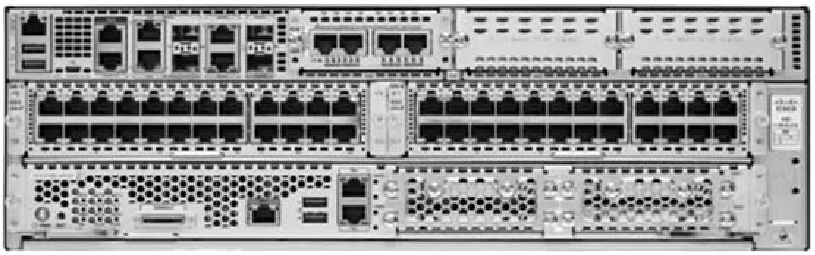
Prime offer nearly 13-15 categories of report in report launch pad. Such report are useful to monitor and take preventive measure on overall performance of network devices.



Bottom N Device Availability Report

Device IP Address	Device Name	Avg Availability(%)
172.16.15.247	LIBRARY_ACCESS.gcoea.ac.in	93.67
172.16.15.240	STAFF_QTR.gcoea.ac.in	97.42
172.16.15.243	GIRLS_HOSTEL.gcoeamravati.local	97.42
172.16.15.241	GIRLS_HOSTEL_NEW.gcoeamravati.local	97.42
172.16.15.244	PRINCIPAL_HOUSE.gcoeamravati.local	99.5
172.16.15.252	GCOEA_DATACENTER_POE.gcoeamravati.local	100.0
172.16.15.250	COMPUTER_ENGG.gcoeamravati.local	100.0
172.16.15.248	ENTC.gcoeamravati.local	100.0
172.16.15.254	GCOEA-CORE-1.gcoeamravati.local	100.0
172.16.15.249	INFORMATION_TECH.gcoeamravati.local	100.0
172.16.15.246	CIVIL_ACCESS.gcoeamravati.local	100.0
172.16.15.245	GCOEA_VOICE_ROUTER.gcoeamravati.local	100.0

***Any availability loss is due to power failures at respective departments.



Cisco ISR4321 Integrated Service Router

Product overview

The Cisco® 4000 Series Integrated Services Routers (ISR 4000) revolutionize WAN communications in the enterprise branch. With new levels of built-in intelligent network capabilities and convergence, they specifically address the growing need for application-aware networking in distributed enterprise sites. These locations tend to have lean IT resources. But they often also have a growing need for direct communication with both private data centers and public clouds across diverse links, including Multiprotocol Label Switching (MPLS) VPNs and the internet.

The ISR 4000 Series contains the following platforms: the 4461, 4451, 4431, 4351, 4331, 4321, and 4221 ISRs.

In our campus we have used the router to install Communication Management Express that enables the Voice Register Global on the router for installing IP phones. Using available devices as per tender we have deployed them and established an intercom network using IP phones. In order to call local, national, international and mobile numbers it is mandatory to have PRI lines connected to router. We have already informed the CWN in-charge regarding the requirement of lines. On availability of lines we confirm to configure the lines.

The show running configuration of router is as below:

```
GCOEA_VOICE_ROUTER#show running-config

Building configuration...

Current configuration : 13169 bytes

!

! Last configuration change at 13:34:40 IST Wed Jul 14 2021 by admin

! NVRAM config last updated at 13:41:18 IST Wed Jul 14 2021 by admin

!

version 16.6

service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
hostname GCOEA_VOICE_ROUTER
boot-start-marker
boot-end-marker
!
vrf definition Mgmt-intf
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
! card type command needed for slot/bay 0/1
!
no aaa new-model
clock timezone IST 5 30
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 source-interface GigabitEthernet0/0/0
 profile "CiscoTAC-1"

  active

  destination transport-method http

  no destination transport-method email

!

ip nbar http-services

!

ip name-server 172.16.31.10

ip domain name gcoeamravati.local

!

ip dhcp pool VOICE_VLAN_DHCP

 network 10.0.10.0 255.255.255.0

 default-router 10.0.10.1

 option 150 ip 10.0.10.1

!

ip dhcp pool DATA_VLAN_DHCP

 network 10.0.20.0 255.255.255.0

 default-router 10.0.20.1

 dns-server 8.8.8.8 172.16.31.1

!

subscriber templating

!

multilink bundle-name authenticated

!
```

```
crypto pki trustpoint SLA-TrustPoint
 enrollment terminal
 revocation-check crl
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
!
crypto pki certificate pool
 cabundle nvram:ios_core.p7b
!
voice service voip
 allow-connections sip to sip
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
 sip
  bind control source-interface GigabitEthernet0/0/0.10
  bind media source-interface GigabitEthernet0/0/0.10
  registrar server expires max 1200 min 300
  g729 annexb-all
!
voice register global
 mode cme
 source-address 10.0.10.1 port 5060
 max-dn 20
 max-pool 20
 authenticate register
 authenticate realm all
 tftp-path flash:
 create profile sync 0551222145122551
 auto-register
 !
voice register dn  1
 number 912
!
voice register dn  2
 number 916
!
voice register dn  3
 number 911
!
voice register dn  4
 number 917
!
voice register dn  5
 number 913
!
```

```
voice register dn  6
 number 914
!
voice register dn  7
 number 915
!
voice register dn  8
 number 918
!
voice register dn  9
 number 919
!
voice register dn  10
 number 920
!
voice register dn  11
 number 921
!
voice register dn  12
 number 922
!
voice register dn  13
 number 923
!
```

```
voice register dn  14

 number 924

!

voice register dn  15

 number 925

!

voice register pool  1

 busy-trigger-per-button 2

 id mac CC7F.75A7.E87E

 type 7821

 number 1 dn 1

 username user1 password cisco

!

voice register pool  2

 id mac 4CA6.4D12.D779

 type 3905

 number 1 dn 2

 username user2 password cisco

!

voice register pool  3

 busy-trigger-per-button 2

 id mac CC7F.75A7.E7C8

 type 7821

 number 1 dn 3
 username user3 password cisco
!
voice register pool  4
 id mac 4CA6.4D12.9F3C
 type 3905
 number 1 dn 4
 username user4 password cisco
!
voice register pool  5
 busy-trigger-per-button 2
 id mac CC7F.75A7.E7CB
 type 7821
 number 1 dn 5
 username user5 password cisco
!
voice register pool  6
 busy-trigger-per-button 2
 id mac CC7F.75A7.E7FB
 type 7821
 number 1 dn 6
 username user6 password cisco
!
voice register pool  7
 busy-trigger-per-button 2
 id mac CC7F.75A7.E8DE

 type 7821

 number 1 dn 7

 username user7 password cisco

!

voice register pool  8

 id mac 4CA6.4D12.D5DA

 type 3905

 number 1 dn 8

 username user8 password cisco

!

voice register pool  9

 id mac 4CA6.4D12.D4DE

 type 3905

 number 1 dn 9

 username user9 password cisco

!

voice register pool  10

 id mac 4CA6.4D12.D3BE

 type 3905

 number 1 dn 10

 username user10 password cisco

!

voice register pool  11
```

```
 id mac 4CA6.4D12.D5A7
 type 3905
 number 1 dn 11
 username user11 password cisco
!
voice register pool  12
 id mac 4CA6.4D12.D887
 type 3905
 number 1 dn 12
 username user12 password cisco
!
voice register pool  13
 id mac 4CA6.4D12.D717
 type 3905
 number 1 dn 13
 username user13 password cisco
!
voice register pool  14
 id mac 4CA6.4D12.A0D0
 type 3905
 number 1 dn 14
 username user14 password cisco
!
voice register pool  15
```

```
 id mac 4CA6.4D12.D122
 type 3905
 number 1 dn 15
 username user15 password cisco
!
voice-card 0/4
 no watchdog
!
license udi pid ISR4321/K9 sn FDO24190CW3
license boot level uck9
license smart enable
license smart conversion automatic
diagnostic bootup level minimal
spanning-tree extend system-id
!
username admin privilege 15 secret 5 $1$SARp$XYToaEhPNwQxAgMED/mKh.
!
redundancy
 mode none
!
interface GigabitEthernet0/0/0
 description MGMT_ VLAN
 ip address 172.16.15.245 255.255.255.0
 ip nbar protocol-discovery
 negotiation auto

!

interface GigabitEthernet0/0/0.10

 description VOICE_VLAN

 encapsulation dot1Q 10

 ip address 10.0.10.1 255.255.255.0

!

interface GigabitEthernet0/0/0.11

 description DATA_VLAN

 encapsulation dot1Q 11

 ip address 10.0.20.1 255.255.255.0

!

interface GigabitEthernet0/0/1

 no ip address

 shutdown

 negotiation auto

!

interface Service-Engine0/4/0

!

interface GigabitEthernet0

 vrf forwarding Mgmt-intf

 no ip address

 shutdown

 negotiation auto
```

```
!

ip forward-protocol nd

ip ftp username administrator

ip ftp password

ip http server

ip http authentication local

ip http secure-server

ip http client source-interface GigabitEthernet0/0/0

ip tftp source-interface GigabitEthernet0

ip route 0.0.0.0 0.0.0.0 172.16.15.254

!

ip ssh version 2

!

snmp-server group GCOEA v3 auth

snmp-server community GCOEA RW

control-plane

!

mgcp behavior rsip-range tgcp-only

mgcp behavior comedia-role none

mgcp behavior comedia-check-media-src disable

mgcp behavior comedia-sdp-force disable

!

mgcp profile default

!
```

```
telephony-service
 max-conferences 8 gain -6
 transfer-system full-consult
!
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
ntp server 172.16.31.10
wsma agent exec
!
wsma agent config
wsma agent filesys
wsma agent notif
end
GCOEA_VOICE_ROUTER#
```

Domain controllers Primary and secondary:

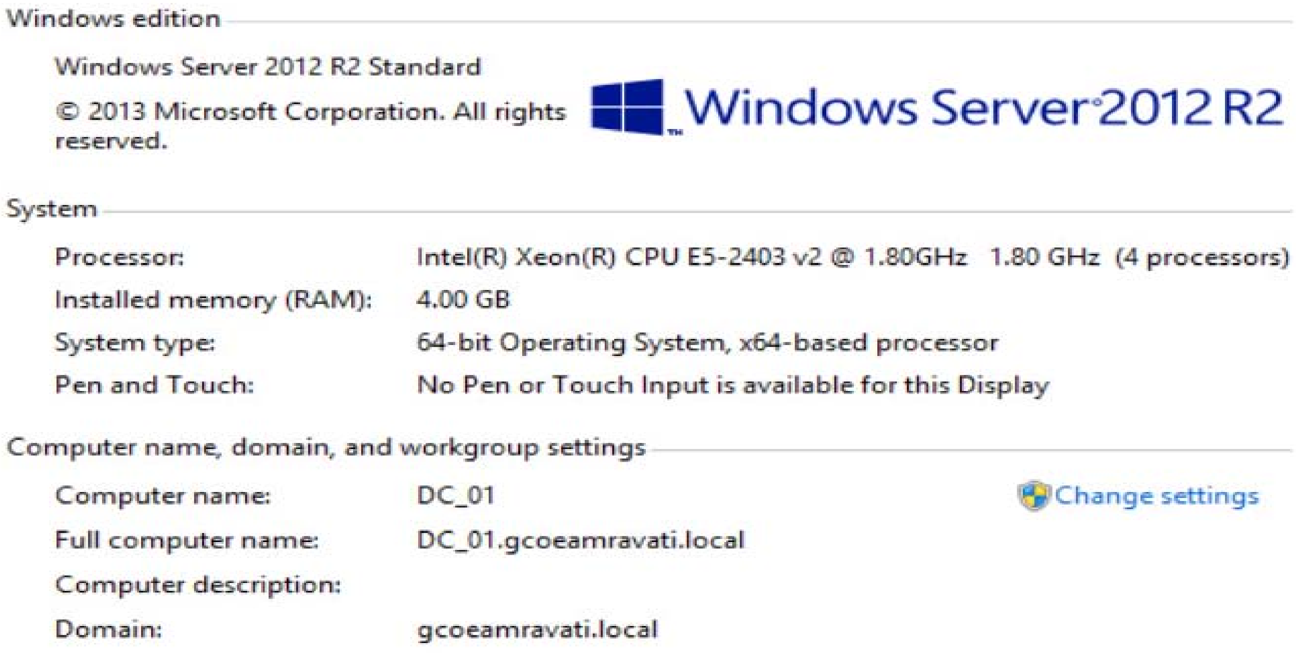
A domain controller is a server that responds to authentication requests and verifies users on computer networks. Domains are a hierarchical way of organizing users and computers that work together on the same network. The domain controller keeps all of that data organized and secured.

The domain controller (DC) is the box that holds the keys to the kingdom- Active Directory (AD). While attackers have all sorts of tricks to gain elevated access on networks, including attacking the DC itself, you can not only protect your DCs from attackers but actually use DCs to detect cyberattacks in progress.

We have instlled primary and secondary domain controllers. We have configured ADDS, DNS, NTP roles in the domain controllers. DHCP for the network is configured in Core switch at datacentre. The primary and secondary domain controller IP address is 192.168.55.11 and 192.168.55.12 respectively. The domain controller name is gcoeamravati.local. To achieve redundancy primary and secondary domain controllers are deployed. If primary domain controller fails then in real time the secondary domain controller is available for the network.

The ADDS, LDAP roles are configured and are ready to be deployed but till date we have not received users list – staff, students and faculty mentioning the first name, last name, email address etc of users. On receipt of user list we will deploy ADDS in the network.

The primary and secondary domain controllers are deployed on HP DL380 server. The server is old with limited compute resources. The server restarts frequently and hence we have not configured DHCP on domain controller. It is recommended to have a new server with required compute resources for seamless deployment of ADDS, DNS in the campus network.



Windows edition

Windows Server 2012 R2 Standard

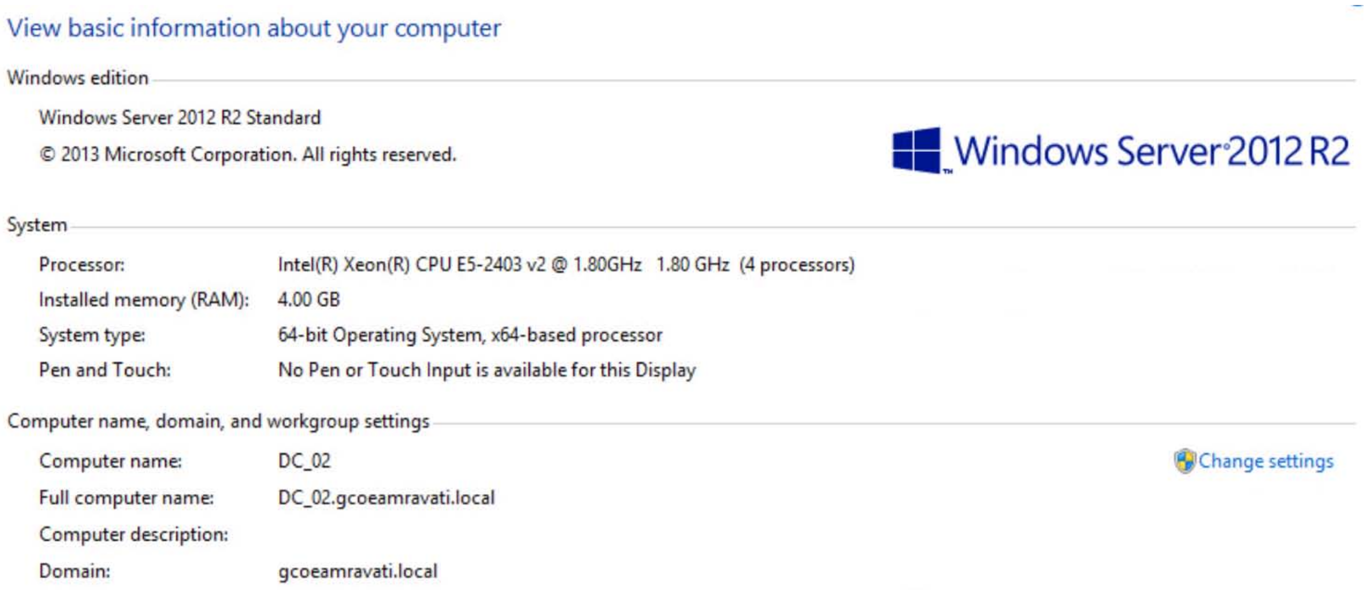
© 2013 Microsoft Corporation. All rights reserved.

System

Processor:	Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz 1.80 GHz (4 processors)
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	DC_01
Full computer name:	DC_01.gcoeamravati.local
Computer description:	
Domain:	gcoeamravati.local



View basic information about your computer

Windows edition

Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

System

Processor:	Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz 1.80 GHz (4 processors)
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	DC_02
Full computer name:	DC_02.gcoeamravati.local
Computer description:	
Domain:	gcoeamravati.local

CERTIFICATE CISCO PRODUCTS

This is to certify/confirm that Cisco items supplied are as per purchase order and are manufactured by Original Equipment Manufacturer (OEM) Cisco only.

IP Scheme Policy:

Category: Cisco Interfaces and Modules		
Category: Routers		
Product Series	**Device Name**	**Device IP Address**
Cisco 4300 Series Integrated Services Routers	GCOEA_VOICE_ROUTER.gcoeamravati.local	172.16.15.245
Category: Switches and Hubs		
Product Series	**Device Name**	**Device IP Address**
Cisco Catalyst 9200 Series Switches	CIVIL_ACCESS.gcoeamravati.local	172.16.15.246
Cisco Catalyst 9200 Series Switches	COMPUTER_ENGG.gcoeamravati.local	172.16.15.250
Cisco Catalyst 9200 Series Switches	ENTC.gcoeamravati.local	172.16.15.248
Cisco Catalyst 9200 Series Switches	GCOEA_DATACENTER_POE.gcoeamravati.local	172.16.15.252
Cisco Catalyst 9200 Series Switches	GIRLS_HOSTEL.gcoeamravati.local	172.16.15.243
Cisco Catalyst 9200 Series Switches	GIRLS_HOSTEL_NEW.gcoeamravati.local	172.16.15.241
Cisco Catalyst 9200 Series Switches	INFORMATION_TECH.gcoeamravati.local	172.16.15.249
Cisco Catalyst 9200 Series Switches	LIBRARY_ACCESS.gcoea.ac.in	172.16.15.247
Cisco Catalyst 9200 Series Switches	PRINCIPAL_HOUSE.gcoeamravati.local	172.16.15.244
Cisco Catalyst 9200 Series Switches	STAFF_QTR.gcoea.ac.in	172.16.15.240
Cisco Catalyst 9400 Series Switches	GCOEA-CORE-1.gcoeamravati.local	172.16.15.254
Cisco Catalyst 9400 Series Switches	GCOEA-CORE-1.gcoeamravati.local	172.16.15.254

Category: Wireless Controllers		
Product Series		
Cisco 3500 Series Wireless LAN Controller	GCOEA_WLC	172.16.23.251
Category: Cisco Firewall		
Cisco FPR2110	GCOEAFPR	172.16.39.253
Category: VMWARE Esxi	vmware Esxi	172.16.8.10
Category: Cisco Prime	Cisco Prime	172.16.15.251

Category: Domain Controller		
Windows Server 2012r2	DC01.gcoeamravati.local	192.168.55.11
Windows Server 2012r2	DC02.gcoeamravati.local	192.168.55.12

Category: Access Points		
Product Series	**Device Name**	**Device IP Address**
Cisco 1562E Series Unified Access Points	B_ADMIN_TERRACE	172.16.16.42
Cisco 1562E Series Unified Access Points	B_CIVIL_TERRACE	172.16.16.8
Cisco 1562E Series Unified Access Points	B_ENTC_TERRANCE	172.16.16.18
Cisco 1562E Series Unified Access Points	B_GIRLS_HOSTEL_1	172.16.16.36
Cisco 1562E Series Unified Access Points	B_IT_DEPT	172.16.16.10
Cisco 1562E Series Unified Access Points	B_LIBRARY	172.16.16.12
Cisco Catalyst 9120AXI Series Unified Access Points	1_ADMIN_ENTRANCE	172.16.16.16
Cisco Catalyst 9120AXI Series Unified Access Points	2_CIVIL_ENTRANCE	172.16.16.5
Cisco Catalyst 9120AXI Series Unified Access Points	3_IN_ENTC	172.16.16.6
Cisco Catalyst 9120AXI Series Unified Access Points	4_COMPUTER_ENGG	172.16.16.3
Cisco Catalyst 9120AXI Series Unified Access Points	5_COMPUTER_ENGG	172.16.16.2
Cisco Catalyst 9120AXI Series Unified Access Points	6_IT_DEPT	172.16.16.11
Cisco Catalyst 9120AXI Series Unified Access Points	7_IN_LIBRARY	172.16.16.7
Cisco Catalyst 9120AXI Series Unified Access Points	8_GIRLS_HOSTEL_1	172.16.16.34
Cisco Catalyst 9120AXI Series Unified Access Points	8_IN_GIRLSHOSTEL_NEW	172.16.16.35
Cisco Catalyst 9120AXI Series Unified Access Points	INDOOR-9120-AP	172.16.16.17

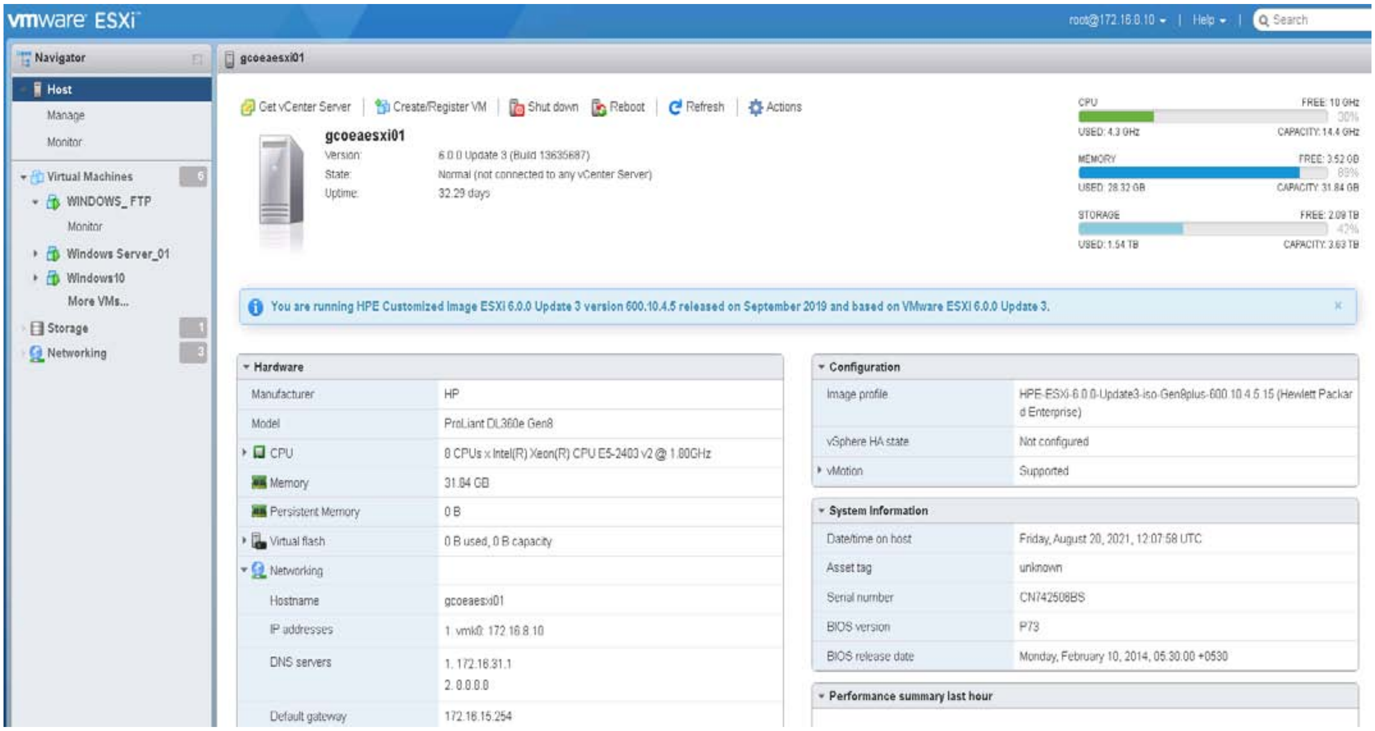
Username and password of all devices & handover of datacenter

Category: Routers			
Product Series	**Device IP Address**	**UserName**	**Password**
Cisco 4300 Series Integrated Services Routers	172.16.15.245	admin	r4321@gcoeaadmin*
Category: Switches and Hubs			
Product Series	**Device IP Address**	**UserName**	**Password**
Cisco Catalyst 9200 Series Switches	172.16.15.246	admin	l2@gcoea246
Cisco Catalyst 9200 Series Switches	172.16.15.250	admin	l2@gcoea103
Cisco Catalyst 9200 Series Switches	172.16.15.248	admin	l2@gcoea248
Cisco Catalyst 9200 Series Switches	172.16.15.252	admin	l2@gcoeaadmin*
Cisco Catalyst 9200 Series Switches	172.16.15.243	admin	l2@gcoeaadmin*
Cisco Catalyst 9200 Series Switches	172.16.15.241	admin	l2@gcoeaadmin*
Cisco Catalyst 9200 Series Switches	172.16.15.249	admin	l2@gcoea249
Cisco Catalyst 9200 Series Switches	172.16.15.247	admin	l2@gcoea247
Cisco Catalyst 9200 Series Switches	172.16.15.244	admin	l2@gcoeaadmin*
Cisco Catalyst 9200 Series Switches	172.16.15.240	admin	l2@gcoeaadmin*
Cisco Catalyst 9400 Series Switches	172.16.15.254	admin	l3@gcoeaadmin*
Cisco Catalyst 9400 Series Switches	172.16.15.254	admin	l3@gcoeaadmin*

Category: Wireless Controllers			
Product Series			
Cisco 3500 Series Wireless LAN Controller	172.16.23.251	admin	Wlclock#254
Category: Cisco Firewall			
Cisco FPR2110	172.16.39.253	admin	Fprlock#253
Category: VMWARE Esxi	172.16.8.10	root	Exsilock#100
Category: Cisco Prime	172.16.15.251	root	Primelock#251
Category: Domain Controller			
Windows Server 2012r2	192.168.55.11	administrator	$P@$$w0rd$
Windows Server 2012r2	192.168.55.12	administrator	$P@$$w0rd$

Vmware Management Console:

The Vmware was duly installed please find below the console image. Warranty details enclosed.



gcoeaesxi01

Version:	6.0.0 Update 3 (Build 13635687)
State:	Normal (not connected to any vCenter Server)
Uptime:	32.29 days

CPU FREE: 10 GHz 30% USED: 4.3 GHz CAPACITY: 14.4 GHz

MEMORY FREE: 3.52 GB 89% USED: 28.32 GB CAPACITY: 31.84 GB

STORAGE FREE: 2.09 TB 42% USED: 1.54 TB CAPACITY: 3.63 TB

You are running HPE Customized Image ESXi 6.0.0 Update 3 version 600.10.4.5 released on September 2019 and based on VMware ESXi 6.0.0 Update 3.

Hardware

Manufacturer	HP
Model	ProLiant DL360e Gen8
CPU	8 CPUs x Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz
Memory	31.84 GB
Persistent Memory	0 B
Virtual flash	0 B used, 0 B capacity
Networking	
Hostname	gcoeaesxi01
IP addresses	1. vmk0: 172.16.8.10
DNS servers	1. 172.16.31.1 2. 0.0.0.0
Default gateway	172.16.15.254

Configuration

Image profile	HPE-ESXi-6.0.0-Update3-iso-Gen9plus-600.10.4.5.15 (Hewlett Packard Enterprise)
vSphere HA state	Not configured
vMotion	Supported

System Information

Date/time on host	Friday, August 20, 2021, 12:07:58 UTC
Asset tag	unknown
Serial number	CN742508BS
BIOS version	P73
BIOS release date	Monday, February 10, 2014, 05:30:00 +0530

Performance summary last hour

Cisco Commerce details regarding mismatch of CON-SNT

CCO USER ID	ambhore.premchand@cisco.com
Date	21.08.2021

Product /Offer Name	Service SKU	Service/Offer Description	Subscription ID/Contract Number	Start Date	End Date	End Customer Name	Qty
CP-3905=	CON-3SNT-CP3905	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-7821-K9=	CON-3SNT-CP7821K9	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
AIR-AP1562E-D-K9	CON-SNT-AIRAP152	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4X-E	CON-SNT-C920024X	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4G-E	CON-SNT-C920L24G	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-3905=	CON-3SNT-CP3905	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-3905=	CON-3SNT-CP3905	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-3905=	CON-3SNT-CP3905	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-3905=	CON-3SNT-CP3905	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-3905=	CON-3SNT-CP3905	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-3905=	CON-3SNT-CP3905	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-3905=	CON-3SNT-CP3905	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-3905=	CON-3SNT-CP3905	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-3905=	CON-3SNT-CP3905	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-7821-K9=	CON-3SNT-CP7821K9	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-7821-K9=	CON-3SNT-CP7821K9	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-7821-K9=	CON-3SNT-CP7821K9	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CP-7821-K9=	CON-3SNT-CP7821K9	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
AIR-AP1562E-D-K9	CON-SNT-AIRAP152	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
AIR-AP1562E-D-K9	CON-SNT-AIRAP152	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1

Product /Offer Name	Service SKU	Service/Offer Description	Subscription ID/Contract Number	Start Date	End Date	End Customer Name	Qty
AIR-AP1562E-D-K9	CON-SNT-AIRAP152	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
AIR-AP1562E-D-K9	CON-SNT-AIRAP152	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
AIR-AP1562E-D-K9	CON-SNT-AIRAP152	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
AIR-AP1562E-D-K9	CON-SNT-AIRAP152	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
AIR-AP1562E-D-K9	CON-SNT-AIRAP152	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
ISR4321-V/K9	CON-3SNT-ISR4321V	3YR SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
FPR2110-NGFW-K9	CON-SNT-FPR21FWN	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4X-E	CON-SNT-C920024X	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4X-E	CON-SNT-C920024X	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4X-E	CON-SNT-C920024X	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4X-E	CON-SNT-C920024X	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4X-E	CON-SNT-C920024X	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4X-E	CON-SNT-C920024X	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4G-E	CON-SNT-C920L24G	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4G-E	CON-SNT-C920L24G	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4G-E	CON-SNT-C920L24G	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9200L-24P-4G-E	CON-SNT-C920L24G	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9404R	CON-SNT-C9404R	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9404R	CON-SNT-C9404R	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
CS-KITPLUS-K9	CON-SNT-CSKITPLU	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
AIR-CT3504-K9	CON-SNT-AIRCTRTK	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1

Product /Offer Name	Service SKU	Service/Offer Description	Subscription ID/Contract Number	Start Date	End Date	End Customer Name	Qty
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
C9120AXI-D	CON-SNT-C9120AXI	SNTC 8X5XNBD	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
L-CME-CUE	CON-ECMU-LCMECEUE	SWSS	203294416	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
R-MGMT3X-N-K9	CON-ECMU-RMGMT3XN	SWSS	203294416	28-Aug-2020	27-Aug-2021	GCOEAMRAVATI	1
A-SPK-EDU		CLD SUPT BASIC 24X7	203486507	24-Aug-2020	23-Aug-2021	GCOEAMRAVATI	1
A-FLEX		CLD SUPT BASIC 24X7	203486507	28-Aug-2020	27-Aug-2023	GCOEAMRAVATI	1
A-FLEX			Sub649074		27-Aug-2023	GCOEAMRAVATI	1
A-SPK-EDU			Sub645779		23-Aug-2021	GCOEAMRAVATI	1

Letter regarding sub-contractor for the CWN project:

Letter as below was duly provided to M/s ACE Computer Solution Amravati regarding appointment as sub-contractor for CWN project with copy to Honorable Principal GCOE Amravati.

ACE COMPUTER SOLUTIONS
Amravati 444601

Date: 14.08.2020
Ref: SCS/2020-21/SAG

Ref: 1. GCOE Amravati Tender No: GCOEA/CWN-DC/2020/553 dated 31.01.2020
2. Purchase Order NO.GCOEAlCWN-DC/2020/1416 dated 27.03.2020
3. Letter No: GCOEA/CWN-DC/2031 dated 22.07.2020
4. Letter No: GCOEA/CWN-DC/2044 dated 23.07.2020
5. Draft Agreement Copy between Shree Comp Systems and GCOEA.

Sub: Sub-contractorship against above referred tender and PO of GCOE Amravati.

Dear Sir,

We write with reference to above mentioned subject and further discussions we are pleased to confirm that your firm M/s ACE Computer Solutions, Agrawal Building, Near Panchsheel Theatre, Amravati 444601 has been appointed as sub-contractor for the contract / project for three years against above referred PO of Government College of Engineering Amravati (GCOE Amravati).

Under the subcontract, ACE Computer Solutions Amravati have to provide on-site services during the installation and support period of three years at GCOE Amravati with one resident engineer at College campus for a period of three years for providing on-site services. The subcontract will also include entire cabling work associated with project / contract, supervision and co-ordination of all activities associated with the contract / project.

The subcontract is subject to:

- Terms and conditions as mentioned in tender, PO and PO extension letter as referred above.
- All terms, conditions and clauses as mentioned in the Agreement to the contract / project between M/s Shree Comp Systems Nagpur and GCOE Amravati.
- Any additional terms and conditions as imposed by the GCOE Amravati during the tenure of contract.

All the above terms, conditions and agreement clauses are applicable to M/s ACE Computer Solutions Amravati during the tenure of contract as a subcontractor.

We will be informing GCOE Amravati regarding appointment of M/s ACE Computer Solutions Amravati as a subcontractor for the contract / project.

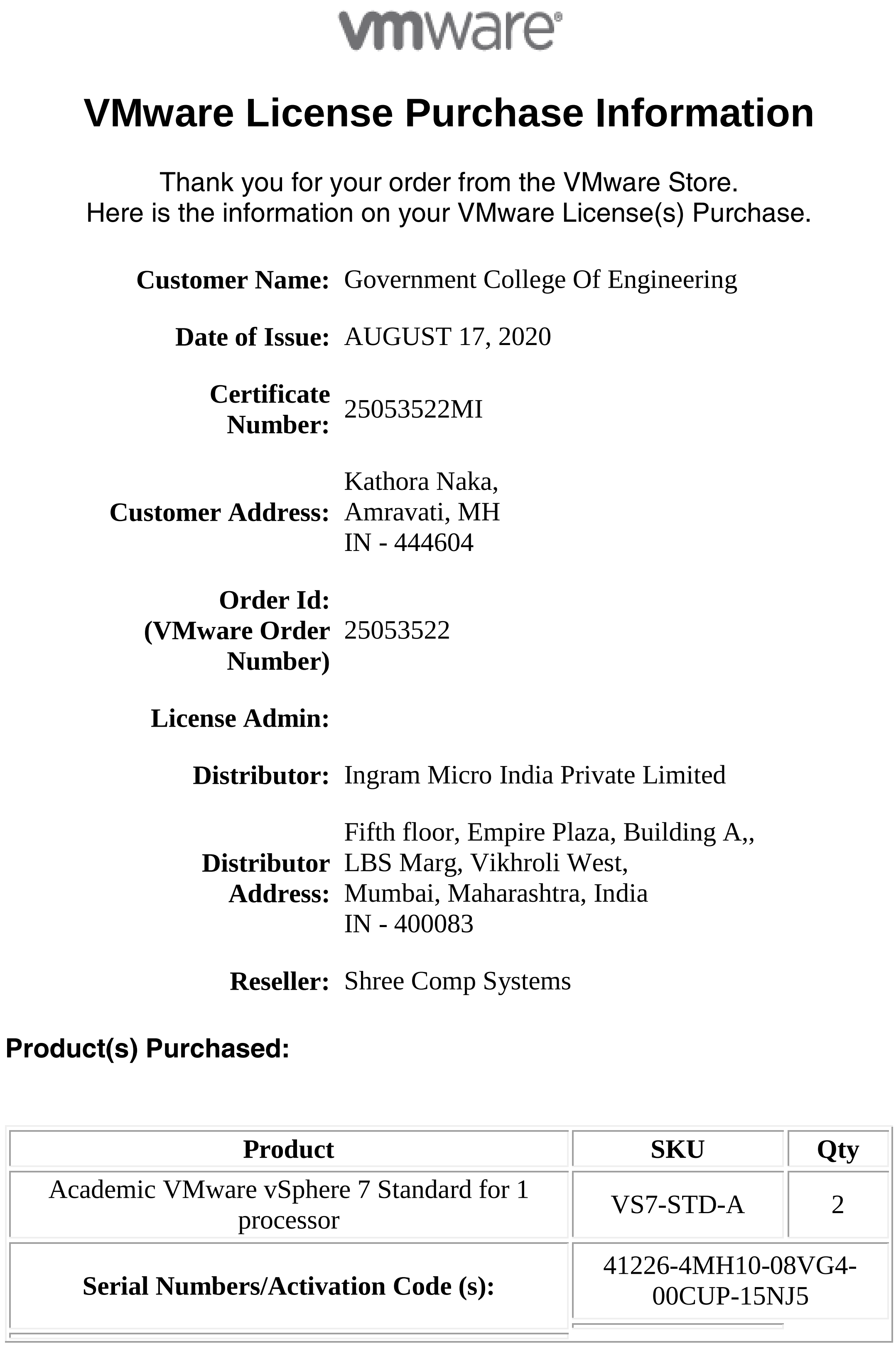
We request you to confirm the acceptance for the same.

Yours faithfully
For Shree Comp Systems

Laxmikant Mahajan
9373109434

Copy to: Principal Sir Government College of Engineering (GCOE) Amravati
Note: All the above terms, conditions and agreement clauses are applicable to M/s ACE Computer Solutions Amravati during the tenure of contract as a subcontractor.
Enclosure: Original Agreement Copy between Shree Comp Systems and GCOE Amravati.

Vmware License:



vmware

VMware License Purchase Information

Thank you for your order from the VMware Store.
Here is the information on your VMware License(s) Purchase.

Customer Name: Government College Of Engineering

Date of Issue: AUGUST 17, 2020

Certificate Number: 25053522MI

Customer Address: Kathora Naka,
Amravati, MH
IN - 444604

Order Id: (VMware Order Number) 25053522

License Admin:

Distributor: Ingram Micro India Private Limited

Distributor Address: Fifth floor, Empire Plaza, Building A,,
LBS Marg, Vikhroli West,
Mumbai, Maharashtra, India
IN - 400083

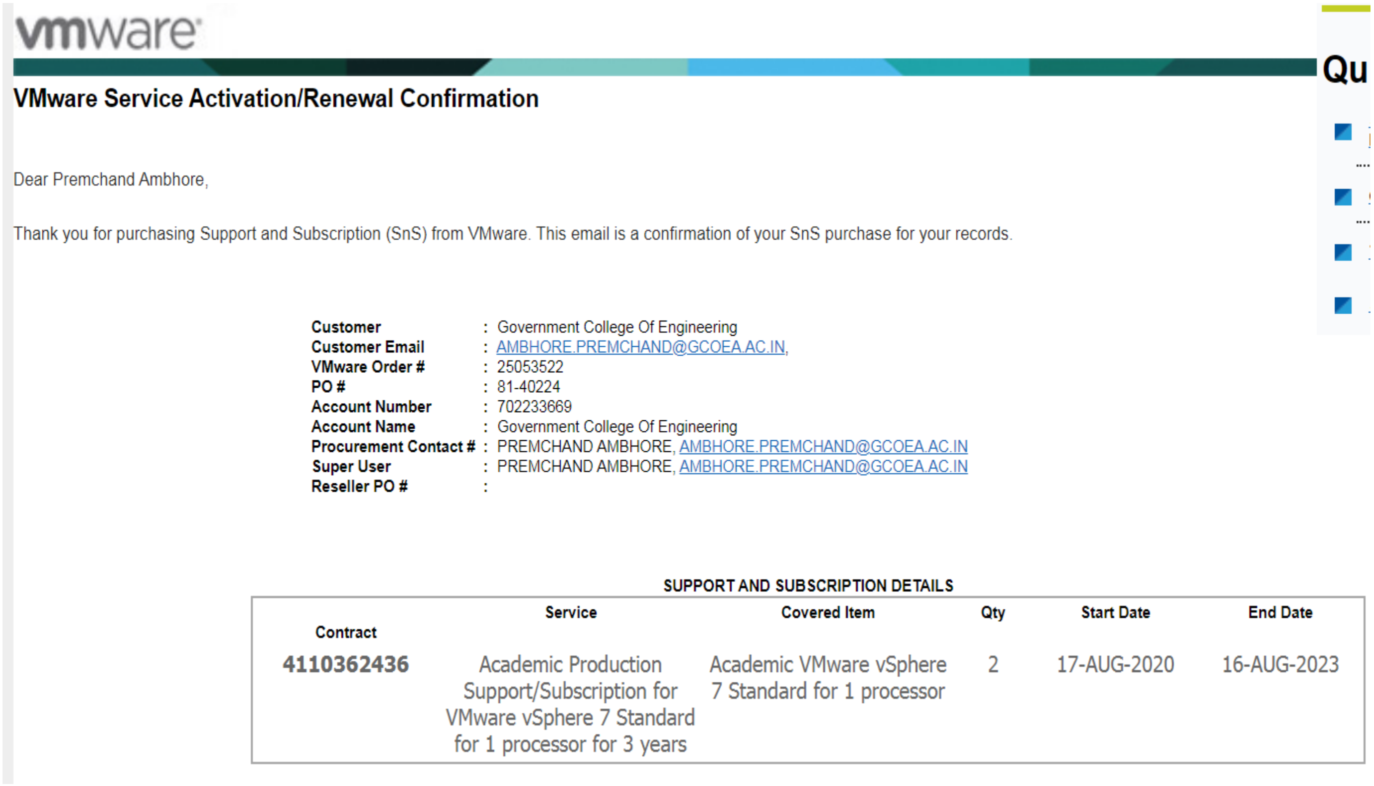
Reseller: Shree Comp Systems

Product(s) Purchased:

Product	SKU	Qty
Academic VMware vSphere 7 Standard for 1 processor	VS7-STD-A	2
Serial Numbers/Activation Code (s):	41226-4MH10-08VG4-00CUP-15NJ5	

VMware International Limited
Parnell House,
Barrack Square,
Ballincollig, Co. Cork,
IRELAND

Vmware Support:



VMware Service Activation/Renewal Confirmation

Dear Premchand Ambhore,

Thank you for purchasing Support and Subscription (SnS) from VMware. This email is a confirmation of your SnS purchase for your records.

Customer	:	Government College Of Engineering
Customer Email	:	AMBHORE.PREMCHAND@GCOEA.AC.IN,
VMware Order #	:	25053522
PO #	:	81-40224
Account Number	:	702233669
Account Name	:	Government College Of Engineering
Procurement Contact #	:	PREMCHAND AMBHORE, AMBHORE.PREMCHAND@GCOEA.AC.IN
Super User	:	PREMCHAND AMBHORE, AMBHORE.PREMCHAND@GCOEA.AC.IN
Reseller PO #	:	

SUPPORT AND SUBSCRIPTION DETAILS

Contract	Service	Covered Item	Qty	Start Date	End Date
4110362436	Academic Production Support/Subscription for VMware vSphere 7 Standard for 1 processor for 3 years	Academic VMware vSphere 7 Standard for 1 processor	2	17-AUG-2020	16-AUG-2023

Cisco Global Technical Services Quick Start Guide

Congratulations on your purchase of a Cisco Technical Services contract!

This Technical Services Quick Start Guide is designed to help you quickly find the information you need to fully use the services to which you are entitled. These
Industry-leading services and support programs can help you proactively maintain network health and operations.
Please read the following information carefully and keep a copy of this guide for future reference. If you require additional information, please contact your Cisco account representative or Cisco reseller. You might want to complete the chart below for ease of reference.

Your Reseller*	SHREE COMP SYSTEMS
End Customer	GOVERNMENT COLLEGE OF ENGINEERING AMRAVATI
Your Contract Number	203294416
Support Start Date	01-JUL-2020
Support End Date	27-AUG-2025

Test certificate of datacenter devices by respective OEMs:

Report and test certificate attached.

LIST OF EQUIPMENTS

INSTALLED

LIST OF EQUIPMENTS INSTALLED

Sr No	Item Description	Unit	Qty	Make
Sr No 2 of BOQ	**Access Control System**			
	2 door controller with suitable enclosure power supply unit	Nos	2	ESSL
	smart card reader with biometric fingerprint cum card type	Nos	2	ESSL
	Smart cards (Blank)	Nos	10	ESSL
	Elctromagnetic lock 600 LBS single leaf with accessories	Nos	2	ESSL
	Emergency door release glass break type	Nos	2	ASES
	Exit switch push button	Nos	2	ESSL
Sr No 3 of BOQ	**Fire Alarm System**			
	1 loop addressable fire alarm panel	No	1	Ravel AVANI
	125 W digital amplifier Evac voice with suitable rack for amplifier		1	Ravel
	Photothermal type smoke detector with std base	Nos	12	Ravel
	Manual call point pull type	Nos	3	Ravel
	Sounder cum strobe	Nos	3	Ravel
	Response indicator	Nos	5	Ravel
	ceiling speaker 6 W	Nos	5	Ravel
Sr No 4 of BOQ	**WLD**			
	2 Zone WLD panel	No	1.00	Jay fire
	15mtr WLD sensor cable	No	1.00	Jay fire
Sr No 5 of BOQ	**Rodent Repellant System**			
	Rodent panel	Nos	1	Jayfire / Synopsys
	Transducer	Nos	10	Jayfire / Synopsys
	Rodent cable	Mtr	75	Jayfire / Synopsys

- Water Leak Detection System
- Rodent Repellent System
- Fire Alarm System

CIN No.: U31908MH2013PTC245823

Synopsys TECH PVT. LTD.

WATER | RODENT | FIRE

T.C.No.: 381/20-21/127 Date: 16.08.2020

TEST CERTIFICATE

Advi Engineering Solutions
PO No. Mail Confirmation PO.Date : 18.08.2020

Inv.No : 127 Inv. Date : 18.08.2020

Product Description	Model No / Make	Qty
Water Leak Detection Panel 2 Zone	Je3523 / Jay	1 Nos

Burn Test

The equipment was switched on & tested periodically for a period of 48 hours at an ambient temperature of approx. 27 degrees. The panels tested OK after this test.

Performance Test.

This is to certify that the panels have been tested as per the client’s specifications. The performance was found to be satisfactory.

Remarks.

IT IS HEREWITH CERTIFIED THAT THE MATERIAL SUPPLIED AGAINST THE ABOVE SAID ORDER ARE SATISFACTORY IN QUALITY, AND IN COMPLIANCE WITH THE REQUIREMENTS SPECIFIED IN THE ORDER.

For **SYNOPSYS TECH PVT LTD.**

SYNOPSYS TECH PVT. LTD. MUMBAI

(Authorized Signatory)

- Water Leak Detection System
- Rodent Repellent System
- Fire Alarm System

CIN No.: U31908MH2013PTC245823

Synopsys TECH PVT. LTD.

WATER | RODENT | FIRE

T.C.No.: 382/20-21/127 Date: 16.08.2020

TEST CERTIFICATE

Advi Engineering Solutions
PO No. Mail Confirmation PO.Date : 18.08.2020

Inv.No : 127 Inv. Date : 18.08.2021

Product Description	Model No / Make	Qty
Water Leak Sensor Cable	WD-CS	15 Mtr

Performance Test.

The performance was found to be satisfactory.

Remarks.

IT IS HEREWITH CERTIFIED THAT THE MATERIAL SUPPLIED AGAINST THE ABOVE SAID ORDER ARE SATISFACTORY IN QUALITY, AND IN COMPLIANCE WITH THE REQUIREMENTS SPECIFIED IN THE ORDER.

Warranty

This is to certify that the above product is under warranty, for a period of 12 month from the date of commissioning or 18 month from the date of supply **whichever is earlier**.

This Warranty Covers the repair or replacement of the Defect / Broken parts at our Discretion.

This certificate does not provide coverage in case of Wrong Installation or Connection or operations of the products from your Ends, and also not for Lost or Destroyed Products.

This Certificate is Void if altered in any way.

For **SYNOPSYS TECH PVT LTD.**

SYNOPSYS TECH PVT. LTD.

(Authorized Signatory)

- Water Leak Detection System
- Rodent Repellent System
- Fire Alarm System

CIN No.: U31908MH2013PTC245823

Synopsys TECH PVT. LTD.

WATER | RODENT | FIRE

T.C.No.: 383/20-21/127 Date: 16.08.2020

TEST CERTIFICATE

Advi Engineering Solutions
PO No.Mail Confirmation PO.Date : 18.08.2020

Inv.No : 127 Inv. Date : 18.08.2020

Product Description	Model No / Make	Qty
Rodent Panel	R-Scat JE 1Z12	1 Nos

Burn Test

The equipment was switched on with full load of 12 Transducers connected individually & tested periodically for a period of 48 hours at an ambient temperature of approx. 27 degrees. The panels tested OK after this test.

Performance Test.

This is to certify that the panels have been tested as per the client's specifications. The performance was found to be satisfactory.

Remarks.

IT IS HEREWITH CERTIFIED THAT THE MATERIAL SUPPLIED AGAINST THE ABOVE SAID ORDER ARE SATISFACTORY IN QUALITY, AND IN COMPLIANCE WITH THE REQUIREMENTS SPECIFIED IN THE ORDER.

For **SYNOPSYS TECH PVT LTD.**

SYNOPSYS TECH PVT. LTD.
MUMBAI

(Authorized Signatory)

- Water Leak Detection System
- Rodent Repellent System
- Fire Alarm System

CIN No.: U31908MH2013PTC245823

Synopsys TECH PVT. LTD.

WATER | RODENT | FIRE

T.C.No.: 384/20-21/127 Date: 16.08.2020

TEST CERTIFICATE

Advi Engineering Solutions

PO No.Mail Confirmation PO.Date : 18.08.2020

Inv.No : 127 Inv. Date : 18.08.2020

Product Description	Model No / Make	Qty
R-Scat Transducer	TRND 150/300	10 Nos

The above mentioned product were tested at our works and they confirm to the specifications, Which are as below.

R-Scat Transducer Specifications:

1) Operating frequence : Above 20 KHz and below 60 Khz.
2) Sound output : 80 dB to 110 dB at 1 meter
3) Power output : 1 W per transducer.
4) Transducer Diemensions : Each Transducer occupies a maximum space of 15 cubic inches.

For **SYNOPSYS TECH PVT LTD.**

SYNOPSYS TECH PVT. LTD. MUMBAI

(Authorized Signatory)

- Water Leak Detection System
- Rodent Repellent System
- Fire Alarm System

CIN No.: U31908MH2013PTC245823

Synopsys TECH PVT. LTD.

WATER | RODENT | FIRE

T.C.No.: 385/20-21/127 Date: 16.08.2020

TEST CERTIFICATE

Advi Engineering Solutions
PO No. Mail Confirmation PO.Date : 18.08.2020

Inv.No : 127 Inv. Date : 18.08.2020

Product Description	Model No / Make	Qty
Rodent Cable	Make R-Scat	50 Mtrs

Performance Test.

The performance was found to be satisfactory.

Remarks.

IT IS HEREWITH CERTIFIED THAT THE MATERIAL SUPPLIED AGAINST THE ABOVE SAID ORDER ARE SATISFACTORY IN QUALITY, AND IN COMPLIANCE WITH THE REQUIREMENTS SPECIFIED IN THE ORDER.

Warranty

This is to certify that the above product is under warranty, for a period of 12 month from the date of commissioning or 18 month from the date of supply **whichever is earlier**.

This Warranty Covers the repair or replacement of the Defect / Broken parts at our Discretion.

This certificate does not provide coverage in case of Wrong Installation or Connection or operations of the products from your Ends, and also not for Lost or Destroyed Products.

This Certificate is Void if altered in any way.

For **SYNOPSYS TECH PVT LTD.**

SYNOPSYS TECH PVT. LTD.

(Authorized Signatory)

RAVEL ELECTRONICS PVT LTD
#150A Electronic Industrial Estate, Perungudi,Chennai - 600 096.
Phone No: 24963241 / 51 | Fax : +91 44 42049599
Email:marketing@ravelfire.com
Website: www.ravelfire.com

Test Certificate

Certificate No. 2100493	Customer Name ADVI ENGINEERING SOLUTIONS		Date 23/07/2021
Invoice No. 2100471	Invoice Date 24/08/2020	Sales Order No. 70510	Customer PO No PO-02 / 20-21

We here by certify that the items detailed hereon have been manufactured , inspected and electrically tested to ensure compliance with Ravel Product and process specification.

Sl No.	Description of Goods	Serial No
1	Model No:AVANIAnalogue Addressable FACP Black - UL Listed - Make: Ravel	RAVNI0LB07000104
2	Model No:AVANI LC Analogue Addressable Loop Card for Avani Panel(Black) - UL Listed - Make: Ravel	RAVNILCN08000381
3	Model No:RE-317D-SHLAddressable Multi Sensor with Base (Smoke & Heat) - UL Listed - Make: Ravel	317M0320-09901-10000
4	Model No:RE-RIResponse Indicator - Make: Ravel	
5	Model No:RE-RIResponse Indicator - Make: Ravel	
6	Model No:RE-RIResponse Indicator - Make: Ravel	
7	Model No:RE-RIResponse Indicator - Make: Ravel	
8	Model No:RE-RIResponse Indicator - Make: Ravel	
9	"Model No:e'Scape, Add. Voice Evac System-16 Z-built-in 230V-125W Digital Amplifier-Make: Ravel"	14180200006
10	Model No:RE-314BIAddressable Isolator Base - Make: Ravel	314BIB0320-05601-05700
11	Model No:RE-716P1TConventional Manual Pull Station - Single Action - UL Listed - Make: Ravel	716R1119-01601-01650

THIS IS A COMPUTER GENERATED DOCUMENT, NO SIGNATURE IS REQUIRED.

Sl No.	Description of Goods	Serial No
12	Model No:RE-717PMBAddressable Back Box with Monitor Module for Manual Pull Station - Make: Ravel	R717PMBR07000594
13	Model No:RE-717PMBAddressable Back Box with Monitor Module for Manual Pull Station - Make: Ravel	R717PMBR07000584
14	Model No:RE-717PMBAddressable Back Box with Monitor Module for Manual Pull Station - Make: Ravel	R717PMBR07000601
15	ModelNo:RE-25SS Conven Wall Mounted Sounder cum Strobe - 100 dBA@1m -Flashing65permin -Make: Ravel	145403-01401-01450
16	Model No:RE-717MCAddressable Control Module - UL Listed - Make: Ravel	R717MCAB07000468
17	Model No:RE-717MCAddressable Control Module - UL Listed - Make: Ravel	R717MCAB07000476
18	Model No:RE-717MCAddressable Control Module - UL Listed - Make: Ravel	R717MCAB07000466
19	"Model No:RE-LS6C, P.A. Speaker - Ceiling Mountable 6W - Tapping: 1.5, 3W and 6W, Col-White"	LS6CCM0320-17131-17140

THIS IS A COMPUTER GENERATED DOCUMENT, NO SIGNATURE IS REQUIRED.

Cisco Global Technical Services Quick Start Guide

Congratulations on your purchase of a Cisco Technical Services contract!

This Technical Services Quick Start Guide is designed to help you quickly find the information you need to fully use the services to which you are entitled. These industry-leading services and support programs can help you proactively maintain network health and operations.

Please read the following information carefully and keep a copy of this guide for future reference. If you require additional information, please contact your Cisco account representative or Cisco reseller. You might want to complete the chart below for ease of reference.

*If applicable.

Your Reseller*	SHREE COMP SYSTEMS
End Customer	GOVERNMENT COLLEGE OF ENGINEERING
Your Contract Number	203294416
Support Start Date	01-JUL-2020
Support End Date	27-AUG-2025

Product Number	PAK/Serial Number	Instance Number	Subscription/Service Level	Start Date	End Date
CP-3905=	FCH2420DW30	5467586150	3SNT	28-Aug-2020	27-Aug-2023
CP-3905=	FCH2420DJDA	5467586154	3SNT	28-Aug-2020	27-Aug-2023
CP-3905=	FCH2420DVHC	5467586156	3SNT	28-Aug-2020	27-Aug-2023
CP-3905=	FCH2420DWX3	5467586158	3SNT	28-Aug-2020	27-Aug-2023
CP-3905=	FCH2420DWJW	5467586160	3SNT	28-Aug-2020	27-Aug-2023
CP-3905=	FCH2420DX51	5467586162	3SNT	28-Aug-2020	27-Aug-2023
CP-3905=	FCH2420DWBG	5467586165	3SNT	28-Aug-2020	27-Aug-2023
CP-3905=	FCH2420DWU7	5467586167	3SNT	28-Aug-2020	27-Aug-2023
CP-3905=	FCH2420DWHD	5467586169	3SNT	28-Aug-2020	27-Aug-2023
CP-3905=	FCH2420DJR6	5467586170	3SNT	28-Aug-2020	27-Aug-2023
CP-7821-K9=	WZP24151R78	5467586490	3SNT	28-Aug-2020	27-Aug-2023
CP-7821-K9=	WZP24151R4E	5467586493	3SNT	28-Aug-2020	27-Aug-2023
CP-7821-K9=	WZP24151QZ5	5467586494	3SNT	28-Aug-2020	27-Aug-2023
CP-7821-K9=	WZP24151QZ2	5467586497	3SNT	28-Aug-2020	27-Aug-2023
CP-7821-K9=	WZP24151R0K	5467586498	3SNT	28-Aug-	27-Aug-

				2020	2023
AIR-AP1562E-D-K9	FGL2421LQY7	5467592320	SNT	28-Aug-2020	27-Aug-2023
AIR-ANT2547VG-N		5467592377	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5467592723	SSTC	26-Jul-2020	25-Jul-2025
AIR-ACC1530-PMK1		5467592455	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E		5467592630	SSTC	28-Aug-2020	27-Aug-2025
WLC-AP-T		5467592837	SSTC	26-Jul-2020	25-Jul-2025
AIR-DNA-E-T		5467592954	SSTC	26-Jul-2020	25-Jul-2025
SWAP1560-LOCAL-K9		5467592546	SNT	28-Aug-2020	27-Aug-2023
AIR-AP1562E-D-K9	FGL2421LQYC	5467592333	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5467592964	SSTC	26-Jul-2020	25-Jul-2025
AIR-DNA-E		5467592644	SSTC	28-Aug-2020	27-Aug-2025
AIR-ANT2547VG-N		5467592388	SNT	28-Aug-2020	27-Aug-2023
SWAP1560-LOCAL-K9		5467592560	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5467592740	SSTC	26-Jul-2020	25-Jul-2025
WLC-AP-T		5467592853	SSTC	26-Jul-2020	25-Jul-2025
AIR-ACC1530-PMK1		5467592466	SNT	28-Aug-2020	27-Aug-2023
AIR-AP1562E-D-K9	FGL2421LQYD	5467592340	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5467592757	SSTC	26-Jul-2020	25-Jul-2025
WLC-AP-T		5467592868	SSTC	26-Jul-2020	25-Jul-2025
SWAP1560-LOCAL-K9		5467592569	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5467592980	SSTC	26-Jul-2020	25-Jul-2025
AIR-DNA-E		5467592655	SSTC	28-Aug-2020	27-Aug-2025
AIR-ANT2547VG-N		5467592396	SNT	28-Aug-2020	27-Aug-2023
AIR-ACC1530-PMK1		5467592474	SNT	28-Aug-2020	27-Aug-2023
AIR-AP1562E-D-K9	FGL2421LQY9	5467592345	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5467592765	SSTC	26-Jul-2020	25-Jul-2025
AIR-ANT2547VG-N		5467592408	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5467592992	SSTC	26-Jul-	25-Jul-

				2020	2025
WLC-AP-T		5467592882	SSTC	26-Jul-2020	25-Jul-2025
SWAP1560-LOCAL-K9		5467592578	SNT	28-Aug-2020	27-Aug-2023
AIR-ACC1530-PMK1		5467592483	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E		5467592670	SSTC	28-Aug-2020	27-Aug-2025
AIR-AP1562E-D-K9	FGL2421LQYB	5467592353	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5467592897	SSTC	26-Jul-2020	25-Jul-2025
PI-LFAS-AP-T		5467592775	SSTC	26-Jul-2020	25-Jul-2025
AIR-ANT2547VG-N		5467592421	SNT	28-Aug-2020	27-Aug-2023
AIR-ACC1530-PMK1		5467592491	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E		5467592687	SSTC	28-Aug-2020	27-Aug-2025
SWAP1560-LOCAL-K9		5467592586	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5467593009	SSTC	26-Jul-2020	25-Jul-2025
AIR-AP1562E-D-K9	FGL2421LQYF	5467592357	SNT	28-Aug-2020	27-Aug-2023
SWAP1560-LOCAL-K9		5467592596	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5467593043	SSTC	26-Jul-2020	25-Jul-2025
AIR-ACC1530-PMK1		5467592503	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5467592909	SSTC	26-Jul-2020	25-Jul-2025
AIR-ANT2547VG-N		5467592433	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E		5467592696	SSTC	28-Aug-2020	27-Aug-2025
PI-LFAS-AP-T		5467592794	SSTC	26-Jul-2020	25-Jul-2025
AIR-AP1562E-D-K9	FGL2421LQYE	5467592362	SNT	28-Aug-2020	27-Aug-2023
AIR-ANT2547VG-N		5467592441	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5467592810	SSTC	26-Jul-2020	25-Jul-2025
SWAP1560-LOCAL-K9		5467592606	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5467592926	SSTC	26-Jul-2020	25-Jul-2025
AIR-DNA-E		5467592705	SSTC	28-Aug-2020	27-Aug-2025
AIR-ACC1530-PMK1		5467592518	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5467593071	SSTC	26-Jul-	25-Jul-

				2020	2025
AIR-AP1562E-D-K9	FGL2421LQY8	5467592371	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5467592941	SSTC	26-Jul-2020	25-Jul-2025
AIR-DNA-E		5467592715	SSTC	28-Aug-2020	27-Aug-2025
AIR-ACC1530-PMK1		5467592530	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5467592825	SSTC	26-Jul-2020	25-Jul-2025
AIR-ANT2547VG-N		5467592447	SNT	28-Aug-2020	27-Aug-2023
SWAP1560-LOCAL-K9		5467592615	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5467593090	SSTC	26-Jul-2020	25-Jul-2025
ISR4321-V/K9	FDO2422M0DC	5467611119	3SNT	28-Aug-2020	27-Aug-2023
CAB-AC-IND		5467611342	3SNT	28-Aug-2020	27-Aug-2023
PVDM4-32	FOC24165MJ5	5467611330	3SNT	28-Aug-2020	27-Aug-2023
MEM-FLSH-4G		5467611181	3SNT	28-Aug-2020	27-Aug-2023
SISR4300UK9-166		5467611345	3SNT	28-Aug-2020	27-Aug-2023
MEM-4320-4G		5467611200	3SNT	28-Aug-2020	27-Aug-2023
SL-4320-IPB-K9		5467611337	3SNT	28-Aug-2020	27-Aug-2023
PWR-4320-POE-AC	PST2349Y0G1	5467611267	3SNT	28-Aug-2020	27-Aug-2023
NIM-BLANK		5467611143	3SNT	28-Aug-2020	27-Aug-2023
SL-4320-UC-K9		5467611164	3SNT	28-Aug-2020	27-Aug-2023
NIM-1CE1T1-PRI	FOC24127PJD	5467611300	3SNT	28-Aug-2020	27-Aug-2023
FPR2110-NGFW-K9	JMX2422Z014	5469267384	SNT	28-Aug-2020	27-Aug-2023
SF-F2K-TD6.3-K9		5469267391	SNT	01-Jul-2020	30-Jun-2023
GLC-SX-MMD	OPM24140G47	5469267393	SNT	28-Aug-2020	27-Aug-2023
PWR-CORD-IND-D		5469267387	SNT	28-Aug-2020	27-Aug-2023
FPR2K-CBL-MGMT		5469267399	SNT	28-Aug-2020	27-Aug-2023
FPR2K-SSD100	MSA24056DLT	5469267395	SNT	28-Aug-2020	27-Aug-2023
FPR2K-SSD-BBLKD		5469267402	SNT	28-Aug-2020	27-Aug-2023
C9200L-24P-4X-E	JAE24190L5E	5470634256	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634515	SSTC	28-Aug-	27-Aug-

				2020	2023
C9200L-NW-E-24		5470634321	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634446	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634439	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634285	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634359	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634399	SNT	28-Aug-2020	27-Aug-2023
C9200L-24P-4X-E	JAE24190L3X	5470634262	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634455	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634405	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634461	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634291	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634366	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634522	SSTC	28-Aug-2020	27-Aug-2023
C9200L-NW-E-24		5470634327	SNT	28-Aug-2020	27-Aug-2023
C9200L-24P-4X-E	JAE24190L1L	5470634265	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634466	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634527	SSTC	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634413	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634370	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634472	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634297	SNT	28-Aug-2020	27-Aug-2023
C9200L-NW-E-24		5470634333	SNT	28-Aug-2020	27-Aug-2023
C9200L-24P-4X-E	JAE24190L53	5470634269	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634375	SNT	28-Aug-2020	27-Aug-2023
C9200L-NW-E-24		5470634339	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634418	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634480	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634303	SNT	28-Aug-	27-Aug-

				2020	2023
C9200-STACK-BLANK		5470634484	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634531	SSTC	28-Aug-2020	27-Aug-2023
C9200L-24P-4X-E	JAE24190CTB	5470634273	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634309	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634490	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634423	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634535	SSTC	28-Aug-2020	27-Aug-2023
C9200L-NW-E-24		5470634345	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634495	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634379	SNT	28-Aug-2020	27-Aug-2023
C9200L-24P-4X-E	JAE24190G5J	5470634278	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634427	SNT	28-Aug-2020	27-Aug-2023
C9200L-NW-E-24		5470634351	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634384	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634500	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634504	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634313	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634537	SSTC	28-Aug-2020	27-Aug-2023
C9200L-24P-4X-E	JAE24190FZL	5470634282	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634391	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634318	SNT	28-Aug-2020	27-Aug-2023
C9200L-NW-E-24		5470634356	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634538	SSTC	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634513	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634509	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634434	SNT	28-Aug-2020	27-Aug-2023
C9200L-24P-4G-E	JAE24220C5H	5470634322	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634507	SSTC	28-Aug-	27-Aug-

				2020	2023
C9200L-NW-E-24		5470634364	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634392	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634452	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634344	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634419	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634445	SNT	28-Aug-2020	27-Aug-2023
C9200L-24P-4G-E	JAE24220C7H	5470634326	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634398	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634424	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634347	SNT	28-Aug-2020	27-Aug-2023
C9200L-NW-E-24		5470634368	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634469	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634511	SSTC	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634460	SNT	28-Aug-2020	27-Aug-2023
C9200L-24P-4G-E	JAE24220CDP	5470634329	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634353	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634428	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634481	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634402	SNT	28-Aug-2020	27-Aug-2023
C9200L-NW-E-24		5470634374	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634516	SSTC	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634474	SNT	28-Aug-2020	27-Aug-2023
C9200L-24P-4G-E	JAE24220C78	5470634332	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634408	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634435	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634486	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634357	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-		5470634491	SNT	28-Aug-	27-Aug-

BLANK				2020	2023
C9200L-NW-E-24		5470634378	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634521	SSTC	28-Aug-2020	27-Aug-2023
C9200L-24P-4G-E	JAE24220CEX	5470634338	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634497	SNT	28-Aug-2020	27-Aug-2023
CAB-TA-IN		5470634415	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634361	SNT	28-Aug-2020	27-Aug-2023
C9200L-DNA-E-24		5470634526	SSTC	28-Aug-2020	27-Aug-2023
C9200L-NW-E-24		5470634383	SNT	28-Aug-2020	27-Aug-2023
PWR-C5-BLANK		5470634441	SNT	28-Aug-2020	27-Aug-2023
C9200-STACK-BLANK		5470634501	SNT	28-Aug-2020	27-Aug-2023
C9404R	FXS2420Q6PS	5470634544	SNT	28-Aug-2020	27-Aug-2023
CAB-SABS-C19-IND		5470634682	SNT	28-Aug-2020	27-Aug-2023
C9400-PWR-BLANK		5470634609	SNT	28-Aug-2020	27-Aug-2023
C9400-SSD-NONE		5470634751	SNT	28-Aug-2020	27-Aug-2023
C9400-DNA-A		5470634555	SSTC	28-Aug-2020	27-Aug-2023
PI-LFAS-T		5470634672	SSTC	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634548	SNT	28-Aug-2020	27-Aug-2023
C9400-NW-A		5470634568	SNT	28-Aug-2020	27-Aug-2023
C9400-PWR-2100AC	DTM241501C1	5470634723	SNT	28-Aug-2020	27-Aug-2023
C9400-SUP-1XL	JAE24202DEF	5470634667	SNT	28-Aug-2020	27-Aug-2023
CAB-CON-C9K-RJ45		5470634582	SNT	28-Aug-2020	27-Aug-2023
S9400UK9-1612		5470634598	SNT	28-Aug-2020	27-Aug-2023
C9400-S-BLANK		5470634619	SNT	28-Aug-2020	27-Aug-2023
C9400-PWR-2100AC	DTM2415018N	5470634746	SNT	28-Aug-2020	27-Aug-2023
C9404R	FXS2420Q6QD	5470634545	SNT	28-Aug-2020	27-Aug-2023
C9400-NW-A		5470634575	SNT	28-Aug-2020	27-Aug-2023
C9400-DNA-A		5470634565	SSTC	28-Aug-2020	27-Aug-2023
PI-LFAS-T		5470634678	SSTC	28-Aug-	27-Aug-

				2020	2023
C9400-SSD-NONE		5470634757	SNT	28-Aug-2020	27-Aug-2023
CAB-SABS-C19-IND		5470634688	SNT	28-Aug-2020	27-Aug-2023
C9400-SUP-1XL	JAE24202DJL	5470634658	SNT	28-Aug-2020	27-Aug-2023
C9400-PWR-2100AC	DTM24150134	5470634740	SNT	28-Aug-2020	27-Aug-2023
S9400UK9-1612		5470634604	SNT	28-Aug-2020	27-Aug-2023
CAB-CON-C9K-RJ45		5470634592	SNT	28-Aug-2020	27-Aug-2023
C9400-PWR-2100AC	DTM24150138	5470634733	SNT	28-Aug-2020	27-Aug-2023
C9400-S-BLANK		5470634625	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470634551	SNT	28-Aug-2020	27-Aug-2023
C9400-PWR-BLANK		5470634615	SNT	28-Aug-2020	27-Aug-2023
CS-KITPLUS-K9	FGL2422LLSX	5470729821	SNT	28-Aug-2020	27-Aug-2023
CS-QUADCAM+	FOC2418NVAH	5470730064	SNT	28-Aug-2020	27-Aug-2023
PSU-12VDC-70W-GR+	AF19005F0TSBC	5470729937	SNT	28-Aug-2020	27-Aug-2023
CAB-PRES-2HDMI-GR		5470729982	SNT	28-Aug-2020	27-Aug-2023
BRKT-QCAM-WMK-		5470729944	SNT	28-Aug-2020	27-Aug-2023
PSU-12VDC-70W-GR+	AF19005F0TTBC	5470729923	SNT	28-Aug-2020	27-Aug-2023
CS-CODEC-PLUS+	FOC2418P916	5470729956	SNT	28-Aug-2020	27-Aug-2023
CAB-DV10-8M+		5470729995	SNT	28-Aug-2020	27-Aug-2023
PWR-CORD-IND-B		5470729972	SNT	28-Aug-2020	27-Aug-2023
CS-TOUCH10+	FOC2420N1Q7	5470730159	SNT	28-Aug-2020	27-Aug-2023
AIR-CT3504-K9	FCW2421M09V	5470730123	SNT	28-Aug-2020	27-Aug-2023
AIR-CT3504-SW-8.5		5470730136	SNT	28-Aug-2020	27-Aug-2023
PWR-115W-AC	DAB2346W3KY	5470730254	SNT	28-Aug-2020	27-Aug-2023
CAB-AC-C5-IND		5470730168	SNT	28-Aug-2020	27-Aug-2023
AIR-CT3504-RMNT		5470730150	SNT	28-Aug-2020	27-Aug-2023
C9120AXI-D	FGL2423L3VP	5470732728	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E		5470733985	SSTC	28-Aug-2020	27-Aug-2025
CDNA-E-C9120		5470733654	SSTC	04-Aug-	03-Aug-

				2020	2025
WLC-AP-T		5470734285	SSTC	04-Aug-2020	03-Aug-2025
SW9120AX-CAPWAP-K9		5470733472	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5470734411	SSTC	04-Aug-2020	03-Aug-2025
NETWORK-PNP-LIC		5470733817	SNT	28-Aug-2020	27-Aug-2023
AIR-AP-T-RAIL-R		5470733258	SNT	28-Aug-2020	27-Aug-2023
AIR-AP-BRACKET-1		5470732940	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5470734134	SSTC	04-Aug-2020	03-Aug-2025
C9120AXI-D	FGL2423L3V8	5470732766	SNT	28-Aug-2020	27-Aug-2023
AIR-AP-BRACKET-1		5470732963	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5470734294	SSTC	04-Aug-2020	03-Aug-2025
CDNA-E-C9120		5470733674	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E		5470733997	SSTC	28-Aug-2020	27-Aug-2025
AIR-DNA-E-T		5470734423	SSTC	04-Aug-2020	03-Aug-2025
PI-LFAS-AP-T		5470734151	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-T-RAIL-R		5470733288	SNT	28-Aug-2020	27-Aug-2023
SW9120AX-CAPWAP-K9		5470733492	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470733840	SNT	28-Aug-2020	27-Aug-2023
C9120AXI-D	FGL2423L3VG	5470732783	SNT	28-Aug-2020	27-Aug-2023
AIR-AP-T-RAIL-R		5470733295	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5470734160	SSTC	04-Aug-2020	03-Aug-2025
SW9120AX-CAPWAP-K9		5470733507	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E		5470734011	SSTC	28-Aug-2020	27-Aug-2025
AIR-AP-BRACKET-1		5470732995	SNT	28-Aug-2020	27-Aug-2023
CDNA-E-C9120		5470733685	SSTC	04-Aug-2020	03-Aug-2025
WLC-AP-T		5470734310	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E-T		5470734434	SSTC	04-Aug-2020	03-Aug-2025
NETWORK-PNP-LIC		5470733856	SNT	28-Aug-2020	27-Aug-2023
C9120AXI-D	FGL2423L3VS	5470732793	SNT	28-Aug-	27-Aug-

				2020	2023
NETWORK-PNP-LIC		5470733874	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5470734445	SSTC	04-Aug-2020	03-Aug-2025
CDNA-E-C9120		5470733696	SSTC	04-Aug-2020	03-Aug-2025
PI-LFAS-AP-T		5470734174	SSTC	04-Aug-2020	03-Aug-2025
WLC-AP-T		5470734320	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E		5470734028	SSTC	28-Aug-2020	27-Aug-2025
SW9120AX-CAPWAP-K9		5470733518	SNT	28-Aug-2020	27-Aug-2023
AIR-AP-T-RAIL-R		5470733307	SNT	28-Aug-2020	27-Aug-2023
AIR-AP-BRACKET-1		5470733022	SNT	28-Aug-2020	27-Aug-2023
C9120AXI-D	FGL2423L3VD	5470732803	SNT	28-Aug-2020	27-Aug-2023
SW9120AX-CAPWAP-K9		5470733536	SNT	28-Aug-2020	27-Aug-2023
AIR-AP-BRACKET-1		5470733040	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470733893	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5470734339	SSTC	04-Aug-2020	03-Aug-2025
PI-LFAS-AP-T		5470734198	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E-T		5470734453	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E		5470734040	SSTC	28-Aug-2020	27-Aug-2025
AIR-AP-T-RAIL-R		5470733322	SNT	28-Aug-2020	27-Aug-2023
CDNA-E-C9120		5470733709	SSTC	04-Aug-2020	03-Aug-2025
C9120AXI-D	FGL2423L3U3	5470732816	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470733906	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5470734344	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-T-RAIL-R		5470733338	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5470734473	SSTC	04-Aug-2020	03-Aug-2025
SW9120AX-CAPWAP-K9		5470733551	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E		5470734055	SSTC	28-Aug-2020	27-Aug-2025
PI-LFAS-AP-T		5470734214	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-BRACKET-1		5470733063	SNT	28-Aug-	27-Aug-

				2020	2023
CDNA-E-C9120		5470733719	SSTC	04-Aug-2020	03-Aug-2025
C9120AXI-D	FGL2423L3VJ	5470732839	SNT	28-Aug-2020	27-Aug-2023
SW9120AX-CAPWAP-K9		5470733560	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E		5470734068	SSTC	28-Aug-2020	27-Aug-2025
AIR-AP-T-RAIL-R		5470733363	SNT	28-Aug-2020	27-Aug-2023
AIR-AP-BRACKET-1		5470733094	SNT	28-Aug-2020	27-Aug-2023
CDNA-E-C9120		5470733733	SSTC	04-Aug-2020	03-Aug-2025
PI-LFAS-AP-T		5470734228	SSTC	04-Aug-2020	03-Aug-2025
NETWORK-PNP-LIC		5470733920	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5470734491	SSTC	04-Aug-2020	03-Aug-2025
WLC-AP-T		5470734355	SSTC	04-Aug-2020	03-Aug-2025
C9120AXI-D	FGL2423L3V5	5470732866	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5470734504	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-T-RAIL-R		5470733388	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5470734365	SSTC	04-Aug-2020	03-Aug-2025
PI-LFAS-AP-T		5470734238	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-BRACKET-1		5470733121	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470733932	SNT	28-Aug-2020	27-Aug-2023
SW9120AX-CAPWAP-K9		5470733580	SNT	28-Aug-2020	27-Aug-2023
CDNA-E-C9120		5470733744	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E		5470734080	SSTC	28-Aug-2020	27-Aug-2025
C9120AXI-D	FGL2423L3VK	5470732890	SNT	28-Aug-2020	27-Aug-2023
SW9120AX-CAPWAP-K9		5470733592	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470733943	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5470734372	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E		5470734093	SSTC	28-Aug-2020	27-Aug-2025
CDNA-E-C9120		5470733766	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-T-RAIL-R		5470733403	SNT	28-Aug-	27-Aug-

				2020	2023
AIR-DNA-E-T		5470734518	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-BRACKET-1		5470733146	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5470734250	SSTC	04-Aug-2020	03-Aug-2025
C9120AXI-D	FGL2423L3VF	5470732904	SNT	28-Aug-2020	27-Aug-2023
AIR-AP-BRACKET-1		5470733181	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5470734257	SSTC	04-Aug-2020	03-Aug-2025
SW9120AX-CAPWAP-K9		5470733603	SNT	28-Aug-2020	27-Aug-2023
CDNA-E-C9120		5470733779	SSTC	04-Aug-2020	03-Aug-2025
NETWORK-PNP-LIC		5470733951	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E-T		5470734532	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-T-RAIL-R		5470733417	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5470734382	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E		5470734103	SSTC	28-Aug-2020	27-Aug-2025
C9120AXI-D	FGL2423L3U2	5470732913	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5470734390	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-BRACKET-1		5470733201	SNT	28-Aug-2020	27-Aug-2023
CDNA-E-C9120		5470733796	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E		5470734113	SSTC	28-Aug-2020	27-Aug-2025
AIR-AP-T-RAIL-R		5470733437	SNT	28-Aug-2020	27-Aug-2023
NETWORK-PNP-LIC		5470733959	SNT	28-Aug-2020	27-Aug-2023
SW9120AX-CAPWAP-K9		5470733616	SNT	28-Aug-2020	27-Aug-2023
PI-LFAS-AP-T		5470734266	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E-T		5470734547	SSTC	04-Aug-2020	03-Aug-2025
C9120AXI-D	FGL2423L3VH	5470732927	SNT	28-Aug-2020	27-Aug-2023
SW9120AX-CAPWAP-K9		5470733632	SNT	28-Aug-2020	27-Aug-2023
AIR-DNA-E		5470734123	SSTC	28-Aug-2020	27-Aug-2025
PI-LFAS-AP-T		5470734272	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-BRACKET-1		5470733222	SNT	28-Aug-	27-Aug-

				2020	2023
NETWORK-PNP-LIC		5470733975	SNT	28-Aug-2020	27-Aug-2023
WLC-AP-T		5470734399	SSTC	04-Aug-2020	03-Aug-2025
AIR-DNA-E-T		5470734554	SSTC	04-Aug-2020	03-Aug-2025
CDNA-E-C9120		5470733807	SSTC	04-Aug-2020	03-Aug-2025
AIR-AP-T-RAIL-R		5470733456	SNT	28-Aug-2020	27-Aug-2023
L-CME-CUE		5475939935	ECMU	28-Aug-2020	27-Aug-2023
CME-UL		5475939948	ECMU	28-Aug-2020	27-Aug-2023
R-MGMT3X-N-K9	567VUP3VNZK	5476021126	ECMU	28-Aug-2020	27-Aug-2021
R-PI36-SW-K9		5476021132	ECMU	28-Aug-2020	27-Aug-2021
L-MGMT3X-94XX-K9		5476021138	ECMU	28-Aug-2020	27-Aug-2021
L-MGMT3X-PI-BASE		5476021130	ECMU	28-Aug-2020	27-Aug-2021
L-MGMT3X-92XX-K9		5476021140	ECMU	28-Aug-2020	27-Aug-2021
L-MGMT3X-ISR4-K9		5476021135	ECMU	28-Aug-2020	27-Aug-2021

END OF REPORT

THANK YOU