



About CCTNS :

- **CCTNS is an acronym of Crime & Criminal Tracking Network and Systems.**
- **CCTNS is a Mission Mode Project under the National e-Governance Plan (NeGP) of Govt. of India. Proposed to be implemented in all Police Stations and all Supervisory offices of the country.**
- **Cabinet Committee on Economics Affairs (CCEA) has approved the project on 19.06.2009.**
- **Under the CCTNS Project, as per CCEA note approx. 14,000 Police Stations and 6000 higher offices throughout the country had been proposed to be automated.**

- **About NCRB :**
- The **National Crime Records Bureau**, abbreviated to **NCRB**, is an Indian government agency responsible for collecting and analysing [crime data](#) as defined by the [Indian Penal Code](#) (IPC). NCRB is headquartered in [New Delhi](#) and is part of the [Ministry of Home Affairs](#) (MHA), [Government of India](#).

CCTNS Services & Objectives

1. Police To Police (P2P)

- Crime registration, investigation and prosecution
- Police messaging and alerts
- Database search and dashboard for decision making

2. Police To Citizen (P2C)

- Portal for citizens to track status of registered applications for Passport verification, NOC for lost phone, vehicle theft, licenses of arms, processions etc.
- Portal can be used for flashing details of dead bodies, missing persons and vehicles

3. Police to Government (P2G)

- Periodic crime review dashboard which will be shared with Government
- Transfer of state level data to NCRB for national level crime data consolidation

Objectives of CCTNS & benefits to police personels:-

- ❖ Make the police functioning citizen friendly and more transparent by automating the functioning of police station
- ❖ Improve delivery of citizen-centric services through effective use of ICT (information and communication technology)
- ❖ Provide the Investigation Officers with tools, technology & information to facilitate investigation of crime and detection of criminals.
- ❖ Improve police functioning in various other areas such as law & order, traffic management etc
- ❖ Facilitate interaction and sharing of information among police stations, districts, State/UT headquarters and other police agencies.
- ❖ Assist senior police officers in better management of police force.
- ❖ Keep track of the progress of cases, including in courts.
- ❖ Reduce manual & redundant records keeping.

CCTNS PROJECT BRIEF SUMMARY

- ❖ State - of - Art system that allows access to 'Crime and Criminal information'
- ❖ Aims to connect all Police Stations & Supervisory Offices in Maharashtra and all States with NCRB, New Delhi
- ❖ Control of Crime (prevention and detection) by exchange of Crime & Criminal data 24x7
- ❖ Storage & Analysis of Crime and Criminal data



System Integrator



**Network Connectivity
provider**



**State Program Management
Unit (SPMU)**

About Hardware , Software, Connectivity , Training & SPMU

Major Components in CCTNS		Provided By
1) Hardware	Computer , Monitor , keyboard , mouse, Printer , Lan Switch , UPS , etc	Wipro (Wipro is SI for Software Development , Hardware , Networking Equipment, Site Preparation , Capacity building & handholding etc.
2) Software	CAS 4.5	NCRB
3) Connectivity. (Network Service Provider)	VPNoBB , VSAT & RF Media , MPLS	BSNL
4) Training	RBT =1,10,000 TOT= 8200 System ADMIN=7100	WIPRO & CID PUNE
5) SPMU	1+2 (For managing the overall project implementation)	PWC

Composition Of Hardware

Hardware Description	P.Stn	ACP/ SDPO/ DCP/ Addl SP	SP	CP	Range/ Jt.CP/ Addl.CP/ Special Offices	SCRB	PHQ	PCR/ FSL/ FPB
Desktop	4	3	10	25	4	10	20	1
Multi-Function Copier	1	1	10	25	1	1	20	1
24 Port Unmanaged Switch	1	1	--	--	1	--	--	--
24 Port Managed Switch	--	--	1	--	--	1	--	--
48 Port Managed Switch	--	--	--	1	--	--	1	--
1 KVA UPS	1	1	--	--	1	--	--	1
5KVA UPS	--	--	1	--	--	2	--	--
15KVA UPS	--	--	--	1	--	--	1	--
External HD, Electronic Pen & Digital Camera	1 each							
Site Preparation	Site Preparation would include electrical cabling , LAN Cabling & Earthing							

Site Preparation (done by Wipro)

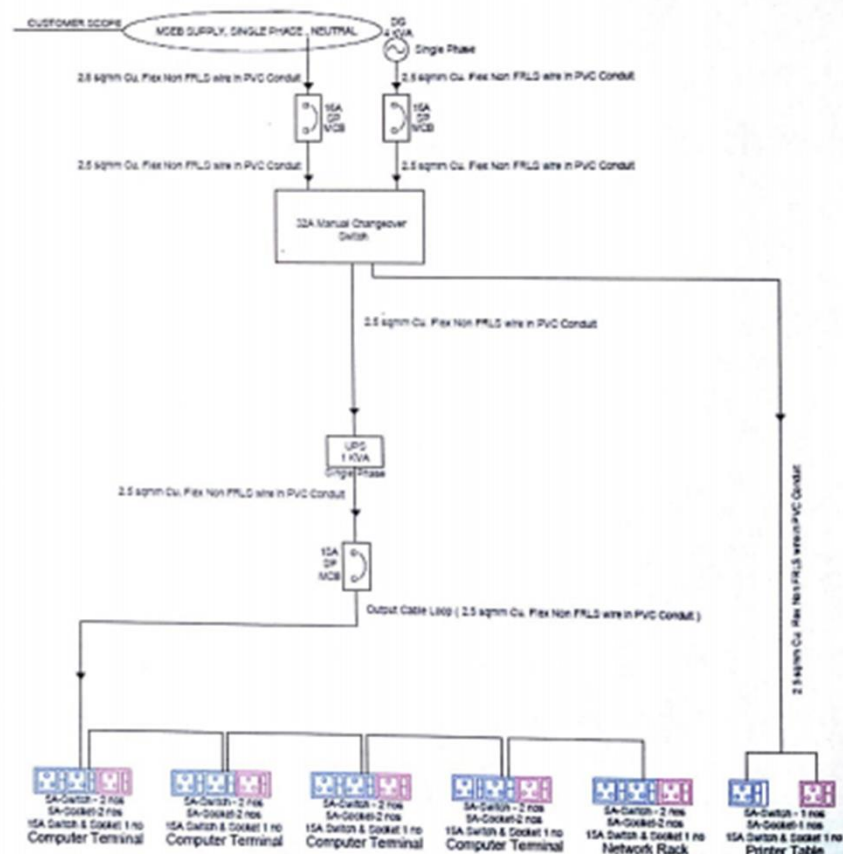
- Site preparation consists of electrical & LAN cabling , installation of rack , switch & panel at all the locations.
- Electrical cabling is done in a way that Online UPS can cater to all the CCTNS computers.
- DG Set is also being provided at all the police stations in order to ensure seamless utilization of CCTNS.
- BSNL modem is being commissioned in the racks & network connectivity ny BSNL is terminated in the modem
- Field officers & CCTNS users should ensure that UPS , CCTNS rack & Modem are always in switched “ON” mode so that health of desktops can be monitored from SDC.



Site Preparation



MAH CCTNS /POLICE STATION SLD WITH 1 KVA UPS



Maharashtra CCTNS Go-Live 15th Sept. 2015

❖ Police Stations enters data in CCTNS from it's Go-Live

❖ **Station Diary**

❖ **Integrated Investigation Forms 1 to 7** [IIF-1 to 7](#)

❖ **Non Cognisable**

❖ **Missing Person**

❖ **Accidental Death**

*** In all the forms the mandatory fields are marked with star (*) signs are to be filled.**

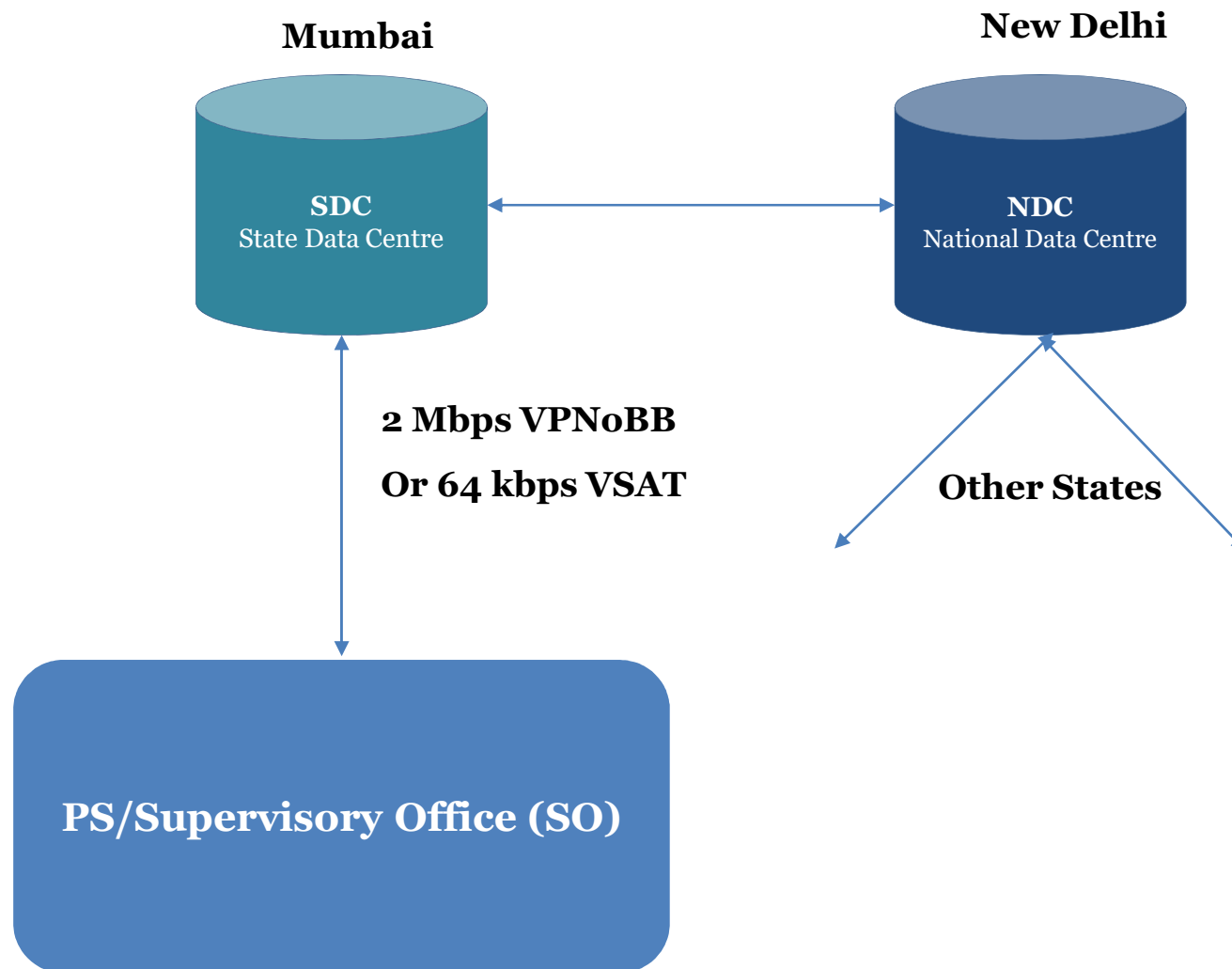
❖ **Records from 1st Jan. 1998 to 15th Sept. 2015 are Migrated** to State Data Centre and after that on line data feeding in being done till date .

All the concerned Officers & Police Personnel Trained under CCTNS Viz. Role Based (1,10,000), Training of Trainers (8200) & System Administrators (7100).
RBTs are still going on for the remaining police personnal.

TOTAL CCTNS SITES IN MAHARASHTRA			
Sr, No	Police Stations	Higher Offices (CP/SP/SDPO/ACP/DCP/ etc)	Total
1	1118	637	1755

Network Connectivity in CCTNS is Provided through the following Types / Modes (at all the 1 755 CCTNS Sites)					
Sr, No	Network Feasibility	Type /Mode Of Connectivity	Police Stations	Higher Offices (CP/SP/SDPO/ACP/DCP/ etc)	Total
1	YES	VPNoBB	1096	633	1729
2	NO	VSAT	21	04	25
3	NO	RF Media	01	--	01
		TOTAL	1118	637	1755

CCTNS Structure

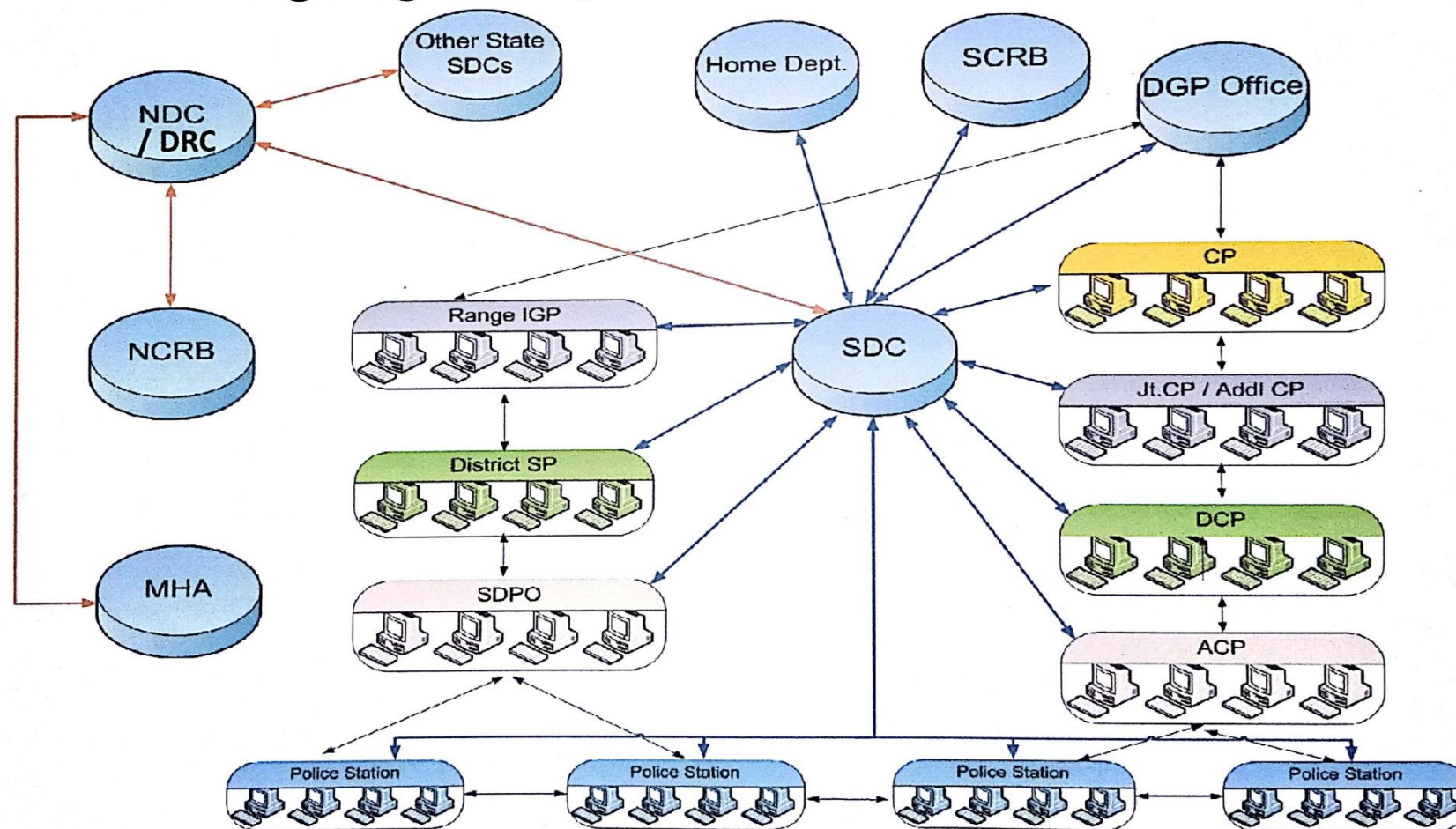




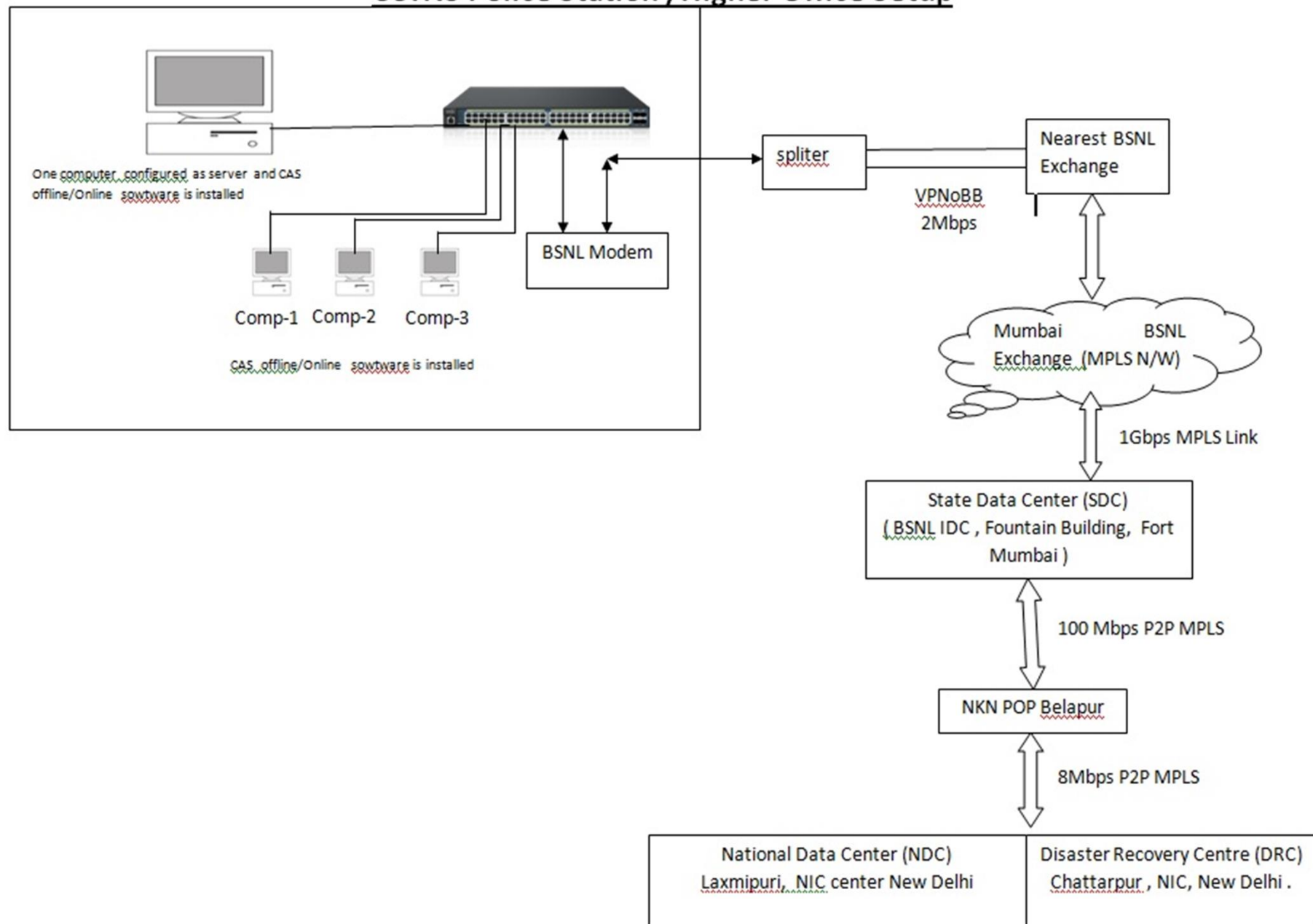
CCTNS Data Flow Diagram



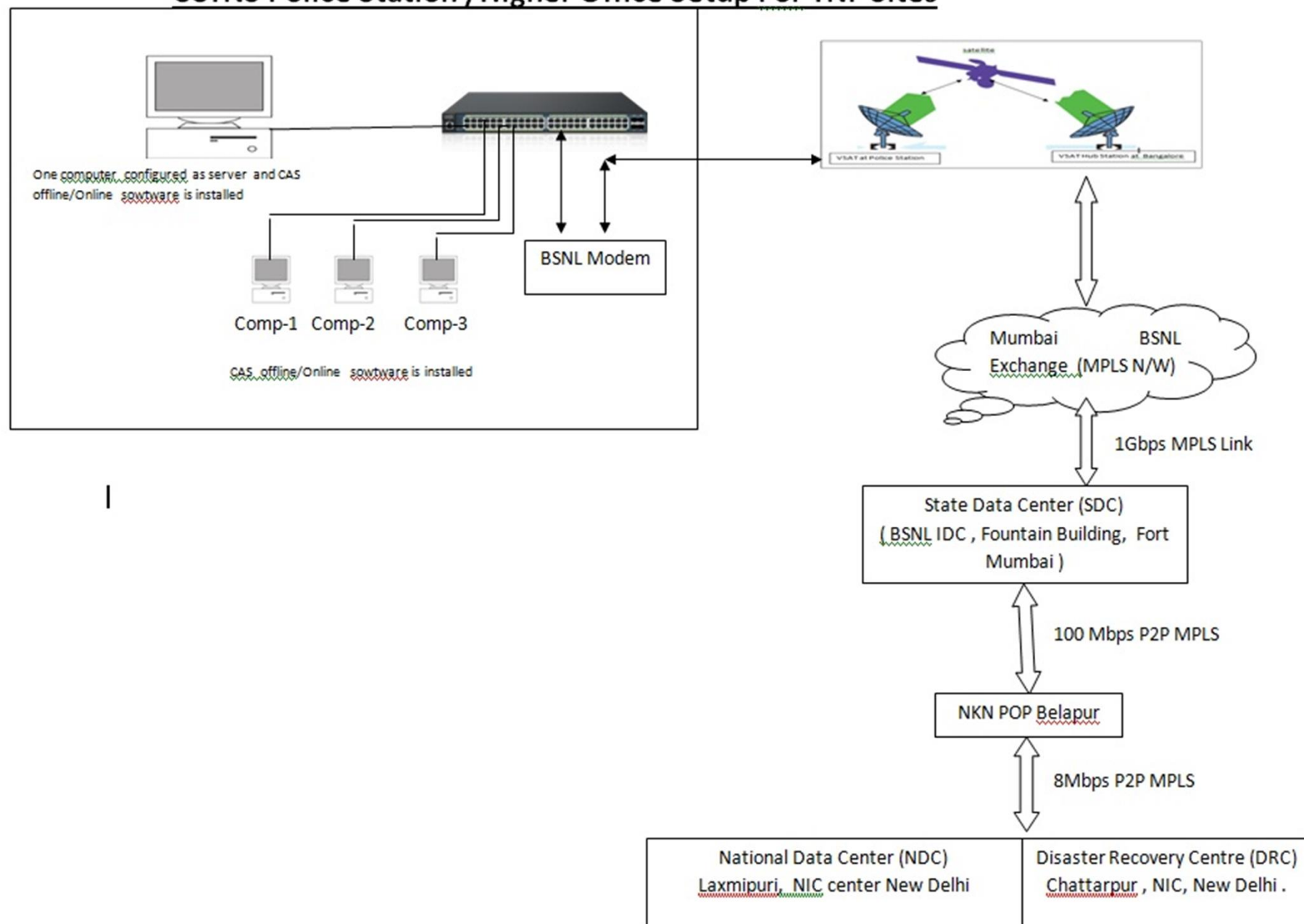
- Following diagram depicts the data flow of CCTNS project



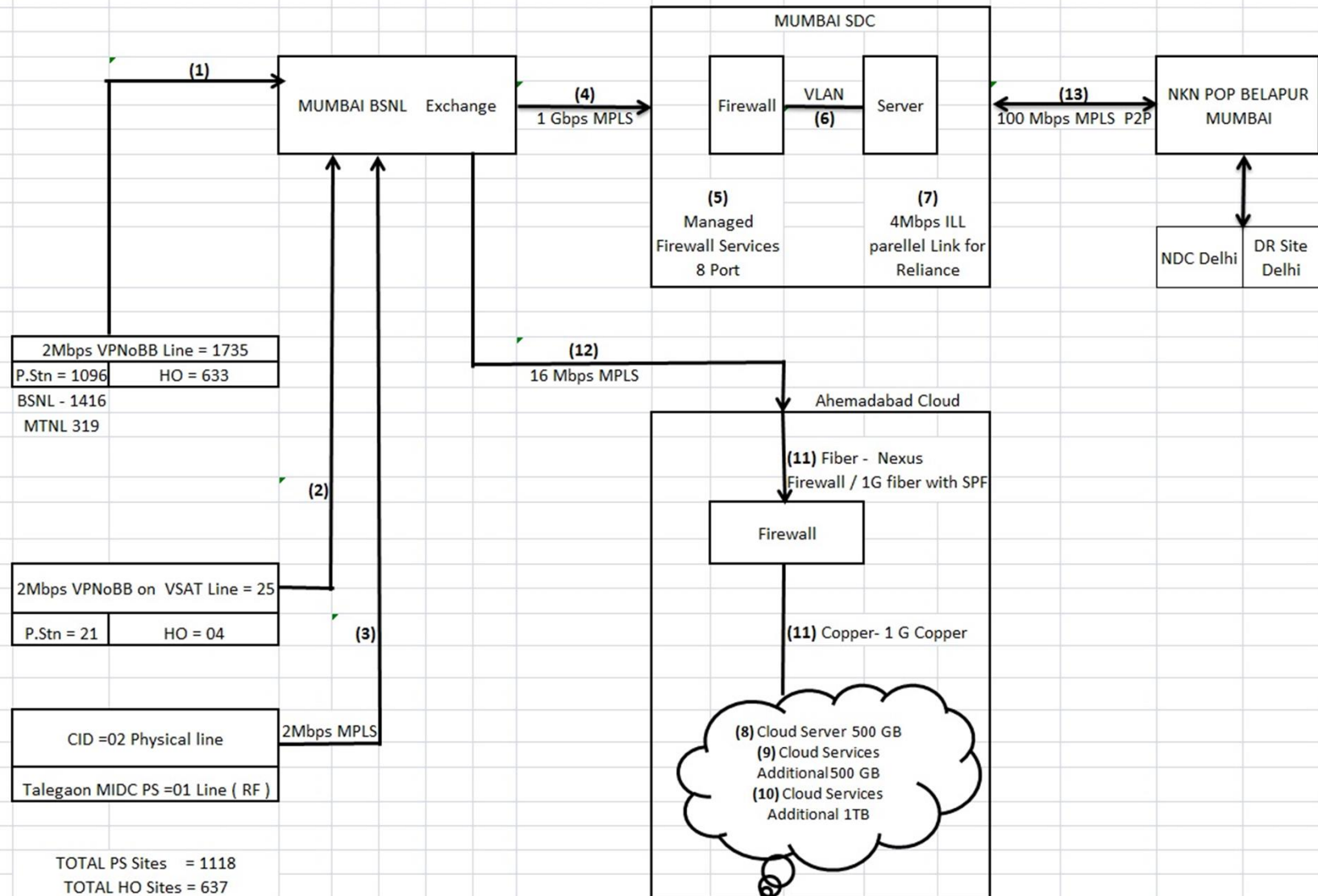
CCTNS Police Station /Higher Office Setup



CCTNS Police Station /Higher Office Setup For TNF Sites



CCTNS Network Block Diagram



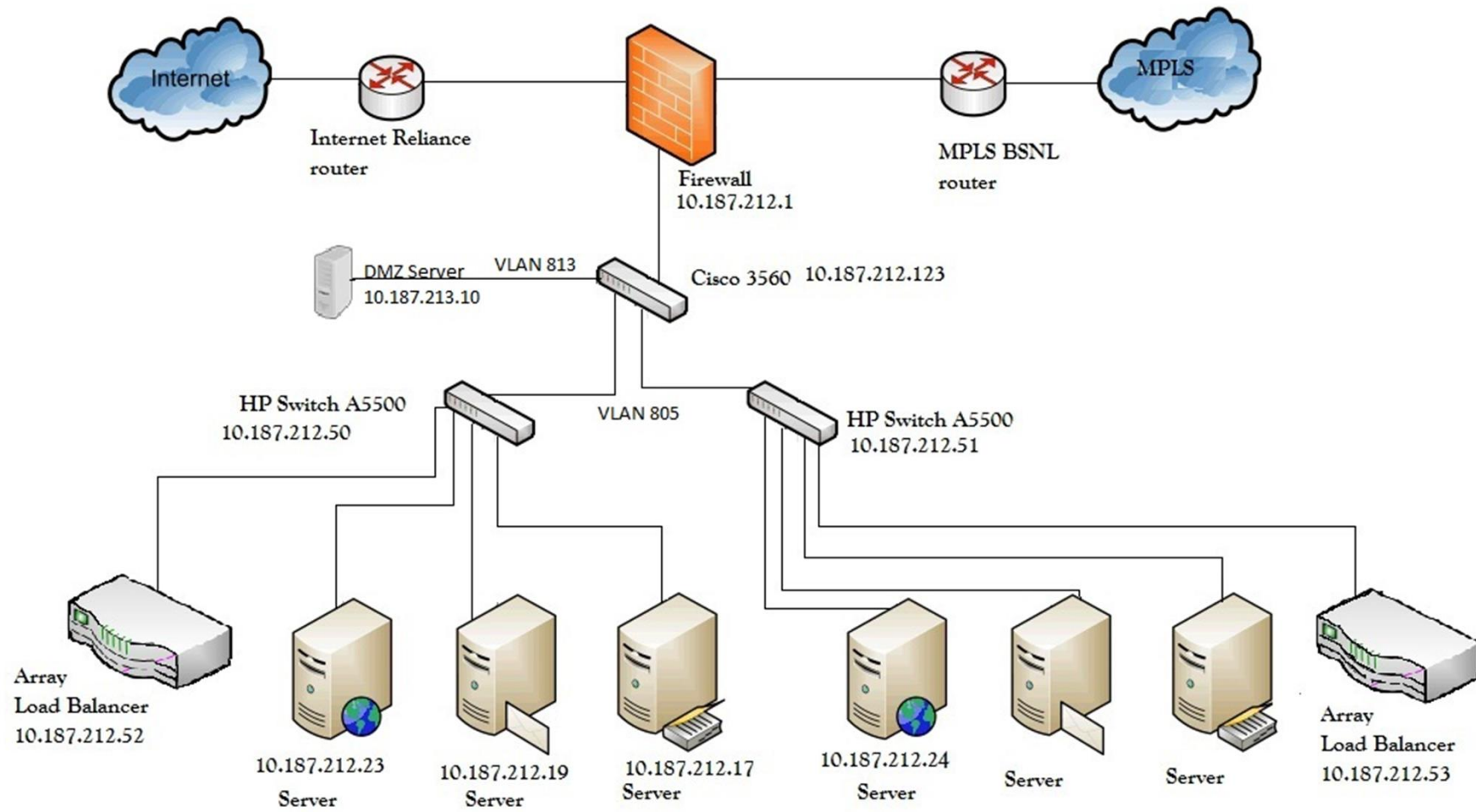
CCTNS HARDWARE :-

- 1) In CCTNS there are two types of Hardware
 - (a) Client Side Hardware
 - (b) Server Side Hardware

Client Side Hardware	Server Side Hardware
All The Hardware supplied to Police Station & Higher Offices is the Client Hardware	Server side hardware consists of storage , networking devices & servers which are housed in SDC & DRC



AT SDC :-



SERVER AVAILABLE AT STATE DATA CENTER

CAS APPLICATION SERVER

ACTIVE DIRECTORY

QMAIL SERVER

NAGIOS MONITORING TOOL

GATEWAY (SMS) & CITIZEN PORTAL

E-HELPLINE TICKETING TOOL

SMTP SERVER

BACKUP SERVER

ANTIVIRUS SERVER

TRAINING SERVER

LOAD BALANCER

Software Used in CCTNS :-

- 1) Operating System :- Ubuntu (Linux Based)
- 2) Web browser :- Mozilla Firefox
- 3) Antivirus :- Calm AV
- 4) Libre Office
 - a. Writer (Word Processor)
 - b. Calc (A spread sheet Program , similar to Microsoft Excel)
 - c. Impress (A presentation similar to Microsoft Power Point .)
 - d. Draw (similar to the diagramming tool similar to Microsoft Visio / Corel draw /DTP)
- 5) CAS (Core Application Software)

ABOUT CAS Application

(A) Brief Overview of CAS (Core Application Software)

CCTNS Solution :- CCTNS is a complex project and is being implemented using “bundle of service” i.e server & client side hardware , software , digitisation , training , maintenance is handled by single System-Integrator ” as against appointing multiple vendors.

The scope of work for- Implementing , commissioning & maintaining in Maharashtra was as follows:-

- **Marathi Customisation of the Core Application Software.**
- **Site preparation at police stations/ Higher offices.**
- **Data center Hardware Installation**
- **End user Hardware Installation at police stations/ Higher Offices.**
- **Networking**
- **Data Digitization of 1 crore + records**
- **Capacity Building & Training of 1 Lakh plus police personnel**
- **Maintenance & support for 5 years post Go-Live**
(Our Go Live Date is 15 Sept 2015) i.e the SI will give us Maintenance support till 15 Sept 2020.

ABOUT CAS Application

(B) Brief Overview of CAS (Online & Offline)

As a part of CCTNS project Implementation :-

- a. CAS 4.5 is made available to Police Station & HO (in Marathi & English)
- b. CAS 4.5 is made available in both online & offline mode.

CAS offline module is deployed at all PStns/HO across the state so that this Offline mode can be used in the event of network connectivity failure for filling the GD and IIF to IIF5 data. Data is automatically synchronized with CAS Online software as and when the network connectivity is established/restored.

CAS On Line Application :-

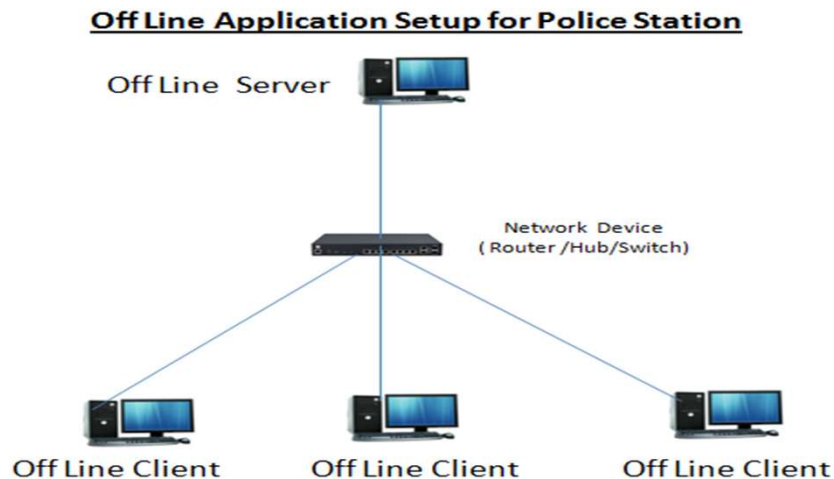
- 1) CAS Online URL of the Live Server where CAS 4.5 application is installed
(URL to Access the CAS Online Server - <http://10.187.212.12/cctnsweb/login.aspx>)**
- 2) All day to day activities to be carried out on CAS online Application like filling GD ,
FIR , Investigation module , prosecution module , & All types of registration form
like missing person , UIDB , prevention etc.**
- 3) We can generate all the reports (State Specific & NCRB reports) registers through
CAS Online Application**
- 4) System Administrators can perform all User related activities & hierarchy mapping
through CAS Online Application.**

CAS Offline Application :-

- 1) CAS Offline application is installed on all desktops provided to the police station**
- 2) CAS Offline application is used , only in case any interruption in Police Station network**
- 3) This helps the police stations to continue their work even in the absence of CAS Online application.**
- 4) Each Desktop has application installed which connects to the Local Server called CAS Offline Server**

Application setup at police station :

- 1) As shown in the diagram , setup is involved 3 desktop (with CAS offline client application installed) and 1 server (CAS offline Server application installed)**
- 2) All clients are connected to Server through LAN connectivity**



Forms Available in CAS :-

The various Forms in CAS are called Integrated Investigation Forms

Sr.No	IIF Forms	Details Of the Forms
1	IIF 1	(FIR)First Information Report
2	IIF 2	Crime Details Form
3	IIF 3	Arrest Form /Court Surrender Form
4	IIF 4	Property Search & Seizure Form
5	IIF 5	Final Form / Final Report
6	IIF6	Court Disposal Form
7	IIF 7	Result Of Appeal Form
8	IIF 8	Missing Person Registration
9		
10	IIF 10	Registration Of Unidentified Dead Body
11	IIF 11	Registration Of Un natural Death
12	OCIS -1	Gang Profile Form
13	OCIS - 2	Gang / Organization Criminal Activity
14	OCIS - 3	Member Detail Form

CAS (Core Application Software) Features

- ❖ Customized Marathi CAS to enter Police Station Diary, Integrated Investigation Forms - IIF 1-7 Forms, Case Diaries etc.
- ❖ Search and view past records (IIF1-7) in respective jurisdiction
- ❖ Generation of Registers viz. crime registers, dead body details, MO, MLC etc.
- ❖ Download and print various state and national reports from CAS
- ❖ Search & query operations to search missing persons, person of interest, property, stolen vehicles etc.
- ❖ SDPOs can view and add remarks on Case Diaries in system

Facilities available to Police

1. Search and Query

- a) Person of Interest Matching (Name Search)
 - b) Status Search (Pendency)
 - c) Property Matching (Abandoned & stolen/involved in case matching)
 - d) Person Matching (Missing & UDB match)
 - e) Quick Search (MOB & Criminal search)
-
- 2. Online Generation and printing of Daily Crime Report (DCR) at P.Stn./District level. 87 Reports available in CAS 4.0
 - 3. Publication of FIRs on website
 - 4. Availability of IIF1 – IIF7 data entry status report
 - 5. SMS to complainant on FIR, Arrest, Charge Sheet submission
 - 6. SMS to senior police officers for visitable offences

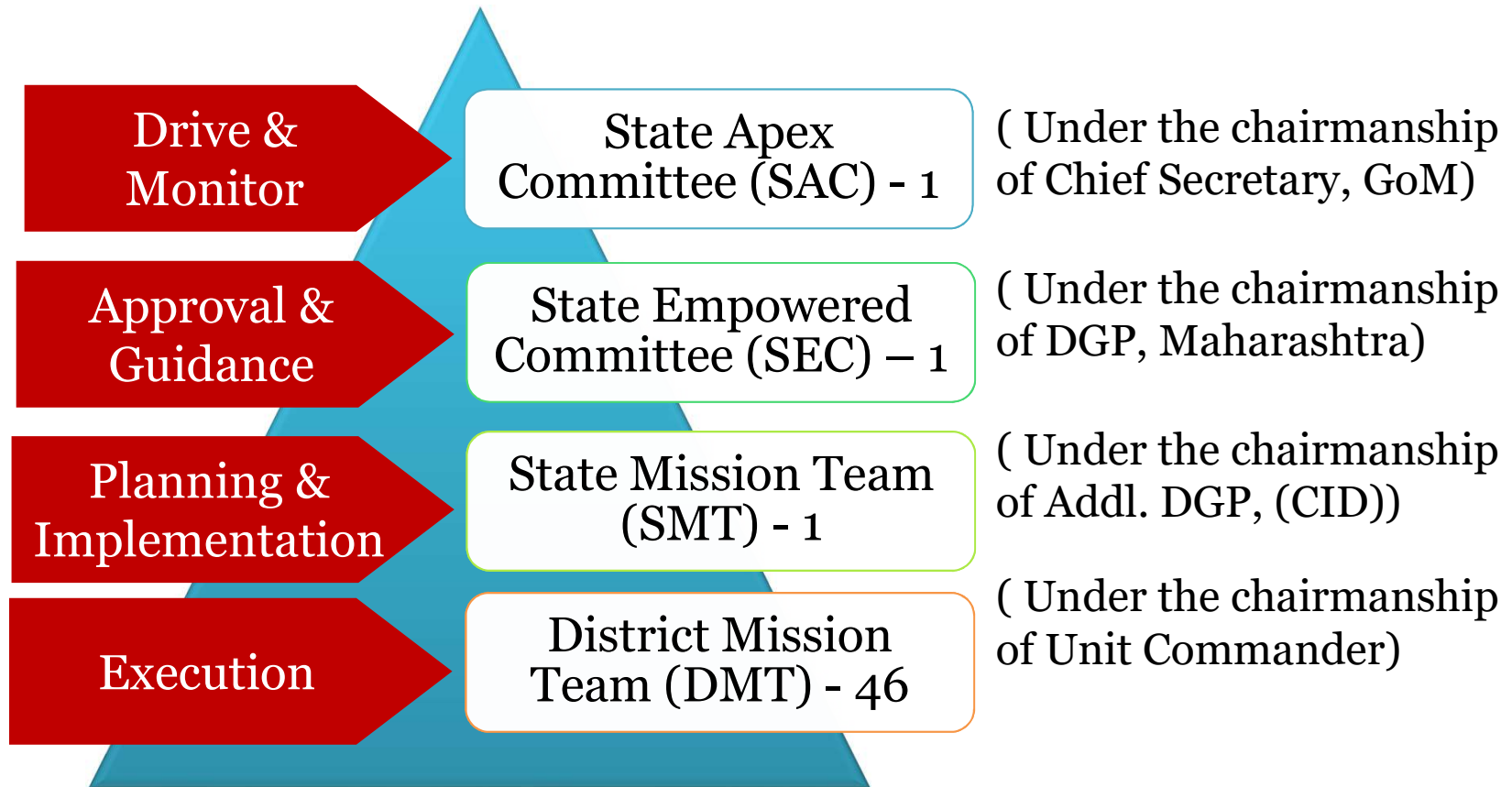
Facilities available to Public on Citizen Portal

- 1) A web portal is made available to citizens with 24 different facilities

Website :- www.mhpolice.maharashtra.gov.in (Go-Live on 7th Jan '16)

- 2) Mobile App Android /ios based is also made available as Citizen Portal is also made available (Go-Live 21 Dec 2017)

CCTNS Governance Structure



Helpdesk BSNL & Wipro:

1. **BSNL Helpdesk: Police** users can lodge complaint related to BSNL link at following numbers.

- a) 1800-345-1500/1504/25634444/25634242/198(Book Fault and take ID No)
- b) IVRS toll free system with automated call response.

2. **Wipro Helpdesk: 6 Days a week. (Sunday closed) – 7 AM to 11 PM**

#	Domain		Whom to Escalate	Whom to Escalate	Whom to Escalate
		Level1	Level2	Level3	Level4
1	CAS Helpdesk	Helpdesk Team	Geeta Sutar Helpdesk Incharge 9762702117 geeta.sutar1@wipro.com	Omkar Shah Project Manager 9820857961 omkar.mahavir@wipro.com	Vishal Patil Program Manager 9833136305 vishal.patil@wipro.com
		020 - 25633308 / 09 / 10			
		cas.helpdesk@wipro.com			
2	Infra Helpdesk	Helpdesk Team	geeta.sutar1@wipro.com	omkar.mahavir@wipro.com	vishal.patil@wipro.com
		020 - 25633308 / 09 / 10			
		infra.helpdesk@wipro.com			

CRIME & CRIMINAL TRACKING NETWORK & SYSTEMS (CCTNS)

- 1) A District Computer Training Centre (DCTC) has been established in all units of Maharashtra State for imparting training to police officers and policemen on basic computer awareness modules as per the syllabus of NCRB, New Delhi. In all, 66 DCTCs are established where training is being imparted to the officers & men on regular basis.
- 2) National Search (CCTNS Search) has started Credentials created for each units
- 4) ICJS (Interoperable Criminal Justice System) : Integration completed recently.
 - a. ICJS is developed by NIC.
 - b. District Admin Credentials created & Police Station Admin Level Credentials creation in process & is almost in completing Phase.
 - c. In future it is also proposed to connect Police , Courts , Prosecution , Prison , Forensic Lab , Finger Print Bureau into an ICJS for facilitating data exchange & search between the various pillars of criminal justice system
- 3) PRISMS (Prison Management System) Integration is in process will be completed soon :
 - a. PRISMS Software is developed by "Goa Electronics Ltd." (it contains 24 Modules)
 - b. Total 41 Prisons in Maharashtra are using this PRISMS Software.
- 5) AMBIS (Automated Multimodal Biometric System) Integration is in process.
- 6) IGR (**Department of Registration & Stamps**) Integration is in process.
- 7) CCTV Integration with CCTNS is in process

Maharashtra CCTNS: Awards & Recognitions

- ❖ **Maharashtra is among leading states across India**
- ❖ **Appreciated by MHA/NCRB, New Delhi in various forums**
- ❖ **Smart Governance Award – 2015 of Govt. of Maharashtra**
- ❖ **SKOCH Smart City National Award, New Delhi – 2015**
- ❖ **ELETS Smart City National Award, New Delhi – 2015**
- ❖ **ELETS Smart City National Award, Bhopal – 2015**
- ❖ **Nasscom National Award for security - 2015**
- ❖ **Govt. of Maharashtra 'Best Capacity Building Award' - 2013**



THANK YOU.

Managed Switch	UNManaged Switch
Managed switches provide all the features of an unmanaged switch and provide the ability to configure, manage, and monitor your LAN. This type of switchse gives you greater control over how data travels over the network and who has access to it. Also, managed switches use protocols such as the Simple Network Management Protocol, or what we call SNMP, for monitoring the devices on the network. SNMP is a protocol that facilitates the exchange of management information between network devices. SNMP queries can determine the health of the network or the status of a particular device. By displaying this data in an easily understood format, IT managers located at a central site can monitor the performance of the network and quickly detect and repair network problems without having to physically interact with the switch	An unmanaged switch simply allows Ethernet devices to communicate with one another, such as a PC or network printer, and those are typically what we call “plug and play.” They are shipped with a fixed configuration and do not allow any changes to this configuration. So an unmanaged switch allows devices to talk to each other, but that is pretty much all that they do?
1) Switch can be configured. 2)Control over Access 3)Control Over LAN 4)SNMP- Allows for Remote Trouble shooting of the Network 5)Expensive 6)Used at Data Centers & Large Sizes enterprises Network	1)Plug & Play with limited configuration like default QoS setting 2)Less Expensive 3)Used at small size bussiness network , home , Lab , conference room etc

Load Balancer :-

1) **Load balancing** refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a *server farm* or *server pool*.

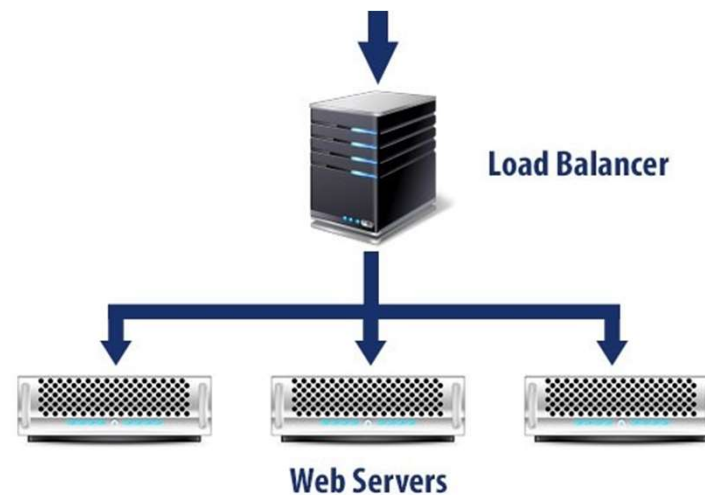
2) A [load balancer](#) acts as the “traffic cop” sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it.

In this manner, a load balancer performs the following functions:

Distributes client requests or network load efficiently across multiple servers

Ensures high availability and reliability by sending requests only to servers that are online

Provides the flexibility to add or subtract servers as demand dictates



Server Monitoring Software :-

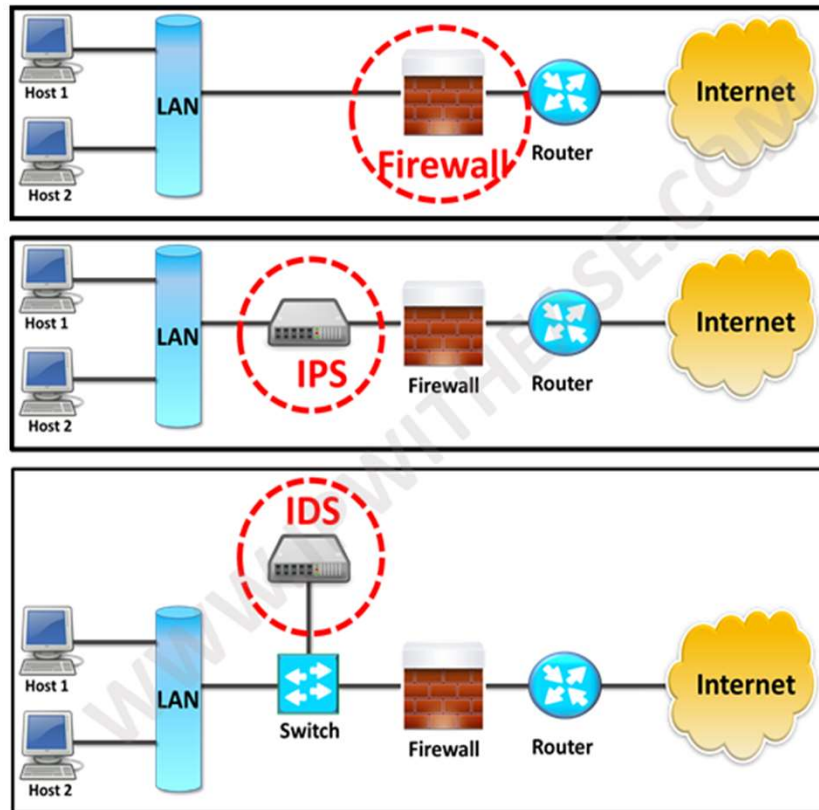
Nagios :- The Industry Standard In IT Infrastructure Monitoring

❖ Nagios Software is known for being the best server monitoring software on the market.

- (1)System Monitoring
- (2)Protocol Monitoring
- (3)Application Monitoring
- (4)Database Monitoring
- (5)Log Monitoring
- (6)Bandwidth Monitoring

FIREWALL VS IPS VS IDS

(i.e Firewall Vs Intrusion Prevention System Vs Intrusion Detection System)



A very common query asked by network and security administrators is difference between **Firewall, IPS and IDS**.

All the 3 terms related to providing security to network and are considered essential components of a Network especially Data Center Network.

The main difference being that firewall preforms actions such as **blocking** and **filtering** of traffic while and IPS/IDS **detects** and **alert** a system administrator or **prevent** the attack as per configuration.

A firewall allows traffic based on set of rules configured. It relies on source, the destination addresses, and the ports. A firewall can deny any traffic that does not meet the specific criteria.

IDS is passive device which watches packets of data traversing the network, comparing with signature patterns and setting off an alarm on detection on suspicious activity. On the contrary, IPS is an active device working in inline mode and prevents the attacks by blocking it.

Furthermore, below table enumerates the difference between **Firewall, IPS and IDS** in detail –

Furthmore, below table enumerates the difference between **Firewall, IPS and IDS** in detail –

Parameter	Firewall	IPS	IDS
Abbreviation for	–	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
Principle of working	Filters traffic based on IP address and port numbers	inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection	Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts
Configuration mode	Layer 3 mode or transparent mode	Inline mode , generally being in layer 2	Inline or as end host (via span) for monitoring and detection
Placement	Inline at the Perimeter of Network	Inline generally after Firewall	Non-Inline through port span (or via tap)
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1 st Line of defense	Should be placed after the Firewall device in network	Should be placed after firewall
Action on unauthorized traffic detection	Block the traffic	Preventing the traffic on Detection of anomaly	Alerts/alarms on detection of anomaly
Related terminologies	- Stateful packet filtering - permits and blocks traffic by port/protocol rules	- Anomaly based detection - Signature detection - Zero day attacks - Blocking the attack	- Anomaly based detection - Signature detection - Zero day attacks - Monitoring - Alarm