RailTel Internship Report

In association with

RailTel Corporation of India Limited

Submitted by

SIBASISH DEY

JAGADISH SAU

SUBARNA MANDAL

SUGATA MONDAL

KUNAL DOLUI

SOUMYAJIT NATH

From

MCKV Institute of Engineering

ACKNOWLEDGEMENT

We are delighted to acknowledge the successful completion of our one-month training cum internship at RailTel Corporation of India Ltd. This enriching experience has been instrumental in broadening our understanding and practical knowledge of Computer Networking and emerging technologies.

We extend our deepest gratitude to Mr. Abhishek Sahay (Assistant General Manager/P&A/ER) for his exceptional guidance and support throughout the internship. His expertise and dedication have been invaluable in providing us with a comprehensive learning experience. We also wish to thank the entire team at RailTel Corporation of India Ltd. for their unwavering support and for creating an environment conducive to learning and professional growth.

The hands-on training we received has significantly enhanced our skills and prepared us to tackle real-world challenges in the field of Computer Networking. We are particularly grateful for the opportunity to work on various projects and technologies that are at the forefront of the industry.

This internship has been a pivotal step in our professional journey, and we are immensely thankful to RailTel Corporation of India Ltd. for this opportunity. We look forward to applying the knowledge and skills we have gained in our future endeavours.

CONTENTS

BASICS OF NETWORKING

ISP:

ISP stands for Internet Service Provider. It is a company or organization that provides access to the Internet for individuals and other entities. Railtel Corporation of India Limited, commonly known as Railtel, functions as an ISP in India primarily through its extensive fiber optic network laid along Indian railways. Here's a concise overview of how Railtel works as an ISP in India:

1. Infrastructure: Railtel owns and operates a vast network of fiber optic cables spanning thousands of kilometers alongside railway tracks across the country.
2. Internet Services: Railtel provides broadband and internet connectivity services to various entities including:
    - Railway Stations: Railtel has implemented high-speed Wi-Fi services at numerous railway stations across India, offering passengers and visitors access to free internet services.
    - Enterprise and Government Clients: Railtel also provides broadband and leased line services to enterprise customers, government agencies, and institutions.
3. Role in Digital India Initiative: Railtel plays a significant role in the Indian government's Digital India initiative by expanding internet access and connectivity to remote and underserved areas through its extensive network infrastructure.
4. Services Offered: Besides internet connectivity, Railtel offers services such as VPN (Virtual Private Network), managed network services, and hosting solutions.
5. Partnerships and Collaboration: Railtel collaborates with various telecom operators, ISPs, and government bodies to extend its reach and enhance service offerings.

Virtualization:

Network virtualization is the process of combining hardware and software network resources and functionalities into a single, software-based administrative entity. This technology abstracts traditional networking functions from the underlying hardware, enabling the creation of multiple virtual networks on a shared physical infrastructure. It allows for the consolidation of physical networks, the subdivision of a single network, and the connection of virtual machines (VMs) together, providing greater flexibility, efficiency, and scalability in managing network resources. Notable examples are:

1. Virtual LANs (VLANs)
2. Software-Defined Networking (SDN)
3. Virtual Private Networks (VPNs)
4. Network Functions Virtualization (NFV)

Telecommunications:

Before telecommunications, long-distance communication was slow and dependent on physical transport methods, like couriers or ships. Technologies like the telegraph allowed messages to travel quickly over long distances. In the early time Samuel Morse invented "Morse Code", this code represents letters and numbers as sequences of dots and dashes. The telegraph machine would convert Morse code characters encoded into electrical impulses or "pulses" that traveled along the wires to the receiving end and at the receiving end, the electrical signals decoded into readable Morse code.

Alexander Graham Bell's Telephone allowing voice transmission over wires converted sound into electrical signals and then back into sound at the receiving end. Traditional telephone systems used analog signals, where voice waves were converted into continuous electrical signals. These signals were transmitted over copper wires or through radio waves. Then radio communication developed where electromagnetic waves used to transmit voice, music, and signals over long distances without any physical connections in radio communication Amplitude Modulation (AM) and Frequency Modulation (FM) methods used for broadcasting audio over radio waves.

In the time of telephone invention the telephones are connected by the copper wires with a centralized exchange office which is allow to connect one end point to another endpoint.

Networking:

Computer networking is the practice of connecting multiple computing devices, such as computers, servers, and mobile devices, to share information and resources. These connections can be established using wired or wireless methods, enabling devices to communicate and collaborate efficiently. Networking allows for the sharing of data, internet access, and peripheral devices like printers, enhancing productivity and connectivity in both personal and professional environments.

1. Network /Computer Networking : -

Networking, or computer networking, is the process of connecting two or more computing devices, such as desktop computers, mobile devices, routers or applications, to enable the transmission and exchange of information and resources. Networked devices rely on communications protocols—rules that describe how to transmit or exchange data across a network—to share information over physical or wireless connections.

Before contemporary networking practices, engineers would have to physically move computers to share data between devices, which was an unpleasant task at a time when computers were large and unwieldy. To simplify the process (especially for government workers), the Department of Defense funded the creation of the first functioning computer network (eventually named ARPANET) in the late 1960s.

Since then, networking practices—and the computer systems that drive them—have evolved tremendously. Today's computer networks facilitate large-scale inter-device communication for every business, entertainment and research purpose. The internet, online search, email, audio and video sharing, online commerce, live-streaming and social media all exist because of advancements in computer networking.

2. Network Protocols :-

A network protocol is a set of rules and conventions that determine how data is transmitted, received, and interpreted across a network. These protocols ensure that different devices, systems, and applications can communicate effectively, regardless of differences in their underlying hardware or software. There are several types of network protocol present such as

- **Transmission Control Protocol (TCP)**: Ensures reliable, ordered, and error-checked delivery of data over the internet.
- Internet Protocol (IP): Responsible for addressing and routing packets of data so they can travel across networks and arrive at the correct destination.
- **Hypertext Transfer Protocol (HTTP)**: Used for transmitting hypertext requests and information on the World Wide Web.

- **Simple Mail Transfer Protocol (SMTP)**: Used for sending and receiving email.
- **File Transfer Protocol (FTP)**: Used to transfer files between a client and a server on a network.

3. IP Addressing and Subnetting:-

- **IP Addressing:** IP (Internet Protocol) addressing is the system used to identify devices on a network. Each device connected to a network is assigned a unique IP address, which acts like a postal address, directing data to the correct location. There are two type IP addressing -
    1. **IPv4:** Uses a 32-bit address format, typically written as four numbers separated by dots (e.g., 192.168.1.1). IPv4 can provide approximately (2^32) unique addresses. However, the actual number is less due to reserved addresses for special purposes (e.g., private networks, multicast). IPv4 is divided into five classes (A, B, C, D, and E) based on the range of the first octet. Classes A, B, and C are used for unicast addressing, D for multicast, and E for experimental purposes.
    2. **IPv6:** Uses a 128-bit address format, written in eight groups of hexadecimal digits (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Pv6 can provide approximately (3.4 x 10^38) unique addresses. IPv6 eliminates the concept of address classes and a more flexible system for subnetting. IPv6 was designed with security and also it reduces the size of routing tables and improves route aggregation and makes the internet's backbone more scalable.

       Actually IPv4 is still widely used due to its long-standing presence, but facing challenges due to limited address space. But more devices come online and the need for a larger address space so new networks and services are being designed to use IPv6 from the start.
- **Subnetting:** Subnetting is the process of dividing a larger network into smaller subnetworks. This improves efficiency and security within a network. Subnetting is often expressed in CIDR (Classless Inter-Domain Routing) notation, which appends a suffix to the IP address indicating the number of bits used for the network portion. This enhances network performance, improves security, and optimizes the use of IP address space. By reducing the size of broadcast domains and segmenting the network, subnetting helps in efficient routing and better organization of network resources.

4. Network Devices :-

❖ Bridges

A network bridge is a device that enables multiple communication networks or network segments to be combined into a single, unified network. This process is referred to as network bridging, which is distinct from routing.

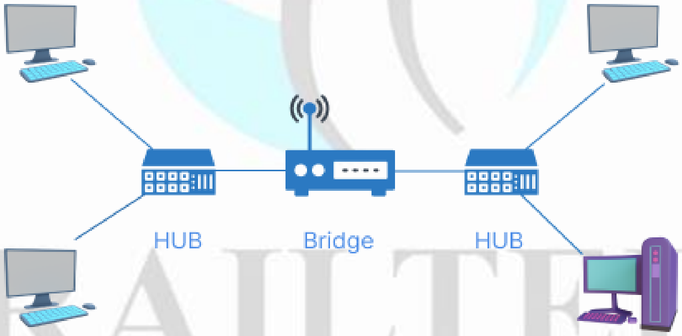
While routing allows multiple networks to communicate independently while remaining separate, bridging connects two separate networks as if they were a single entity. In the OSI model, bridging occurs at the data link layer (layer 2) and is used to connect disparate networks.

When one or more of these segments are wireless, the device is considered a wireless bridge. There are several types of network bridging technologies, including simple bridging, multiport bridging, and learning or transparent bridging.

There are two models in which bridges can be set up in:

Local bridging: where LAN connections are made using local cables.

Remote bridging: where two connections are brought together with a wide area network (WAN).



❖ Hubs

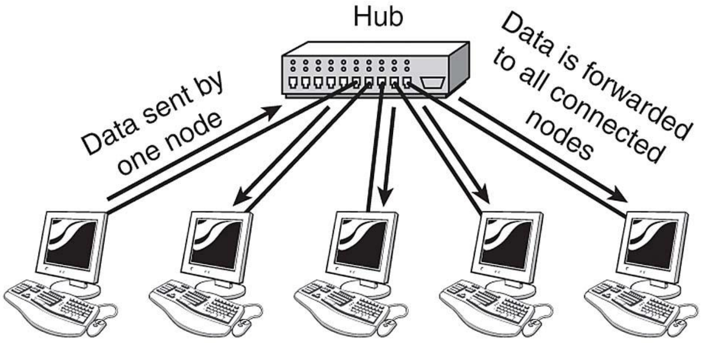
A hub, also known as an active hub or repeater hub, is a network device that connects multiple computer networking devices together, creating a single network segment. It has multiple input/output ports, where a signal introduced at any port is echoed to every other port except the original incoming port.

Operating at the physical layer, a hub works by amplifying and retransmitting incoming signals. Some hubs may also include additional connectors such as BNC or AUI, allowing connection to legacy 10BASE2 or 10BASE5 network segments.

However, hubs are now largely obsolete, having been replaced by network switches in most cases, except in older or specialized installations. In fact, the use of repeaters or hubs to connect network segments is deprecated by the IEEE 802.3 standard, as of 2011.

Hubs come in two types:

- Simple hubs: only one port for connecting a device to other networks.
- Multiple-port hubs: where users can connect to many devices, some of which expand in a modular fashion.



❖ Routers

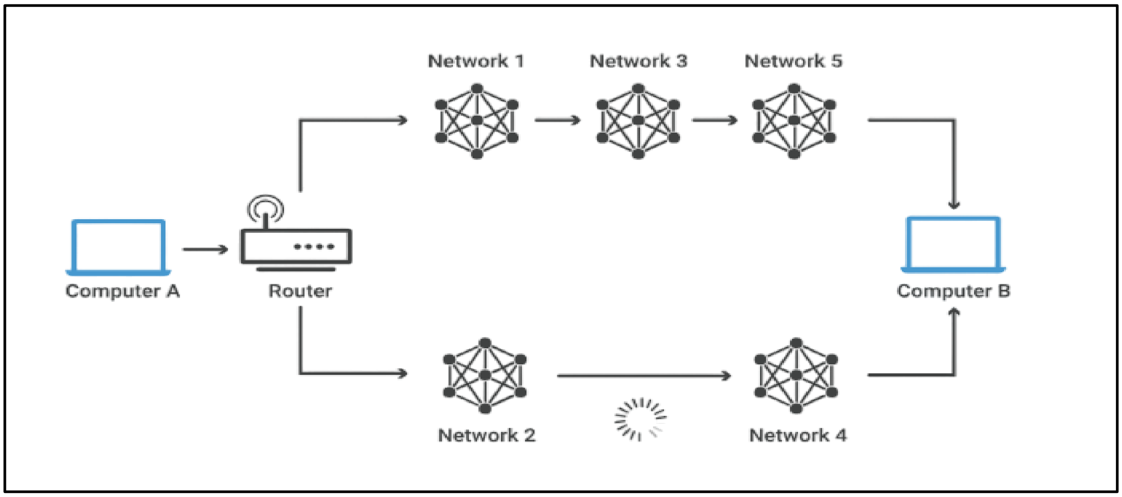
Routers are devices that connect multiple packet-switched networks or subnetworks, performing two primary functions: managing traffic between networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to share the same internet connection.

Typically, most routers serve as a bridge between local area networks (LANs) and wide area networks (WANs). A LAN is a group of connected devices restricted to a specific geographic area, typically requiring a single router.

On the other hand, a WAN is a large network spanning a vast geographic area, often requiring multiple routers and switches due to its distributed nature. Examples of WANs include large organizations and companies with multiple locations across the country, which require separate LANs for each location to form a cohesive network.

Routers can actually be configured as either static or dynamic:

- Static routers: have to be configured manually and will remain static until altered.
- Dynamic routers: will use data from nearby routers to inform their own routing tables.



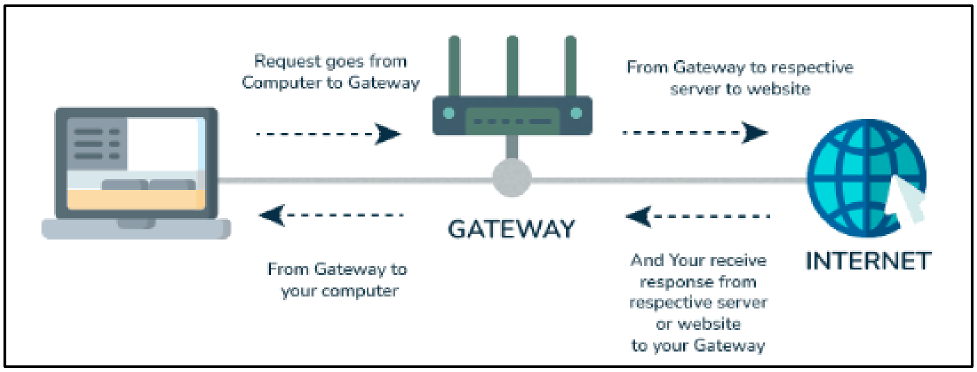
❖ Gateways

A gateway serves as a connection between networks, translating data to enable communication between different networks.

Historically, gateways and routers have been separate devices, but it's becoming more common for them to be combined into a single router. For example, home Wi-Fi routers can act as both a router and a gateway, delivering data within the network while translating it for devices on the receiving end.

A network gateway typically consists of physical components, such as network interface cards and inputs and outputs, as well as software for translating network protocols and providing gateway functions. These functions can be defined, deployed, and controlled through software, and may also be built into other devices, such as routers.

Gateways can be deployed on various layers of the Open Systems Interconnection (OSI) model, but are typically used on the network layer. They can be used in various security processes, including as a firewall or proxy server to scan and filter data, and can be used in either a unidirectional or bidirectional manner, allowing data to flow in only one direction or in both directions.



❖ NICs (Network Interface Cards)

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter, or LAN adapter.

Purpose:-

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale networks through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Types of NIC Cards:-

NIC cards are of two types –

Internal Network Cards:-

In internal network cards, the motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).

External Network Cards:-

In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

❖ Modems

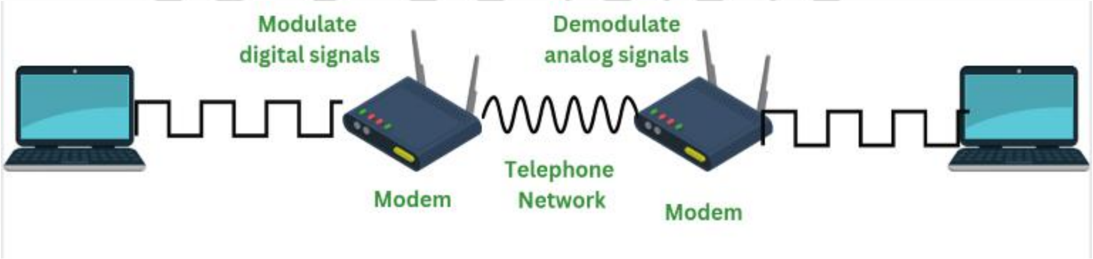
A modem is a crucial piece of computer hardware that converts digital data into a format suitable for transmission over analog mediums, such as phone lines or radio waves. This process involves modulating one or more carrier wave signals to encode the digital information, which is then transmitted over the medium.

The receiver, on the other hand, demodulates the received signal to recreate the original digital information. The ultimate goal of a modem is to produce a signal that can be transmitted efficiently and decoded reliably, regardless of the analog medium being used. In fact, modems can be used with a wide range of analog transmission methods, including light-emitting diodes, radio, and much more.

The receiver, on the other hand, demodulates the received signal to recreate the original digital information. The ultimate goal of a modem is to produce a signal that can be transmitted efficiently and decoded reliably, regardless of the analog medium being used. In fact, modems can be used with a wide range of analog transmission methods, including light-emitting diodes, radio, and much more.

Modems come in three different types:

- DSL modems: often considered the slowest as they use telephone cables.
- Cable modems: faster than DSL because they transmit data over TV lines.
- Wireless modems: the fastest type of transmitter as it transfers information between the local network and an internet service provider (ISP).

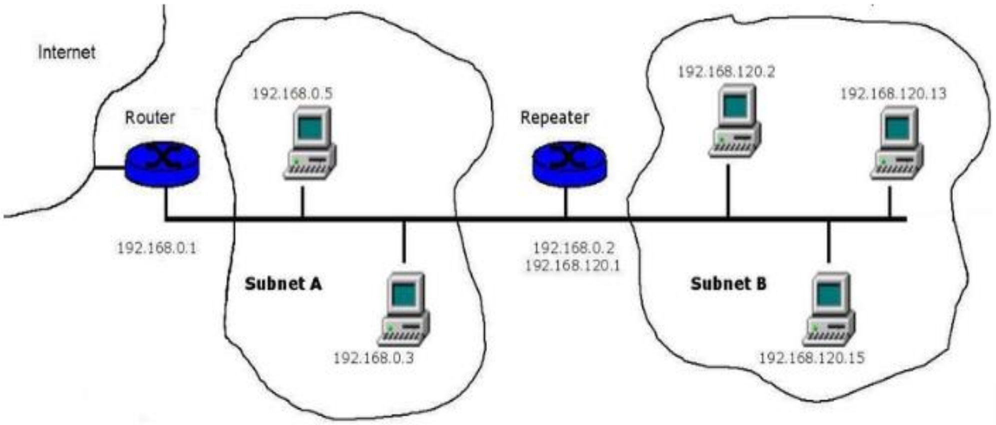


❖ Repeaters

Repeater nodes are a crucial component of computer networks, responsible for amplifying and rebroadcasting incoming signals to extend their reach and make them more usable.

Repeaters are used to increase the network's reach, restore damaged or weak signals, and provide access to nodes that are otherwise inaccessible. They operate by magnifying the received signal to a higher frequency domain, making it more scalable, accessible, and suitable for transmission.

In wired data communication networks, repeaters are employed to extend signal propagation, while in wireless networks, they are used to expand cell size. Additionally, repeaters support a range of transmission types, including analog, digital, and light-based transmissions, making them a versatile and essential component of modern network infrastructure.



5. Network Security:-

Here are some key points about network security:

1. Prevents Unauthorized Access: Ensures that only authorized users can access network resources.
2. Protects Data Integrity: Safeguards data from being altered or tampered with during transmission.
3. Confidentiality: Encrypts data to keep it private and secure from eavesdroppers.
4. Availability: Ensures that network services are available to users when needed, preventing disruptions.
5. Threat Detection and Response: Identifies and responds to suspicious activities and potential threats in real-time.
6. Access Control: Manages who can access what resources within the network.
7. Firewalls and Intrusion Detection Systems (IDS): Uses tools to monitor and control incoming and outgoing network traffic based on predetermined security rules.
8. Regular Updates and Patching: Keeps software and systems up-to-date to protect against known vulnerabilities.

6 (i). Routing:-

Definition: Routing is the process of determining the best path for data to travel from one network to another. Routers analyze the network topology and use routing tables and protocols to direct data packets to their destination across interconnected networks.

Function: Routers connect different networks, such as a local area network (LAN) to a wide area network (WAN), and manage traffic between them. They ensure data is sent efficiently and accurately, often using algorithms to find the optimal path.

6 (ii). Switching:-

Definition: Switching involves moving data packets within the same network. Switches operate at the data link layer (Layer 2) of the OSI model and use MAC addresses to forward data to the correct destination within a local network.

Function: Switches connect multiple devices within a LAN, such as computers, printers, and servers. They manage data traffic by creating a dedicated path for each data packet, reducing collisions and improving network efficiency.

7. Network Performance and Optimization :-

Network optimization is an umbrella term that refers to a range of tools, strategies, and best practices for monitoring, managing, and improving network performance.

In today’s highly competitive, dynamic business environment, it’s not enough for essential networks to perform adequately. As we move further into the digital age, the world depends more and more on reliable, fast, safe, available, 24/7 data transfer. Unfortunately, outdated or under-dimensioned hardware or suboptimal software can limit available bandwidth and introduce increased latency. Obsolete or underutilized network security options can negatively impact performance and leave systems unprotected. Sudden surges or spikes in traffic can overwhelm essential network functions and slow down response times. And the list goes on, creating potentially hundreds of mounting issues capable of deteriorating the end-user experience.

The primary goal of network optimization is to ensure the best possible network design and performance at the lowest cost structure. The network must promote increased productivity and usability and allow data to be exchanged effectively and efficiently. And this is achieved by managing network latency, traffic volume, network bandwidth, and traffic direction.

Benefits of Network Optimization :-

Managed effectively, network optimization is capable of helping organizations build more effective and efficient internal and external networks. This carries with it a number of distinct advantages, including the following:

- **Increased Network Throughput**

  Network optimization removes the hurdles that stand in the way of optimal data transmission speeds. This means decreased latency and jitter, faster response times, and a better-connected IT ecosystem, and, as a result, increased throughput.

- **Enhanced Employee Productivity**

  Latency, packet loss, and downtime in internal networks prevent employees from being able to access and use vital tools and information when and how they need them most. Network optimization keeps data flowing properly, so your workforce doesn’t have to sit on its hands waiting for your network to catch up.

- **Improved Analytics and Security Posture**

  An important element of network analytics and security is traffic visibility. By keeping a close eye on what traffic is moving through your network, where it’s going, and what it’s doing, you’ll gain the benefit of being able to more quickly identify and respond to threats, and track various crucial metrics, including those outlined above.

  Armed with this information, organizations using network performance monitoring and diagnostic (NPMD), application performance monitoring (APM), and security tools can analyze captured data and turn it into valuable, actionable insights. These tools can be further enhanced with advanced metadata, including attributes from the application layer, to solve more advanced use cases. Network analytics can likewise be employed in predictive modeling, providing accurate forecasts of future network usage.

- **Enriched Customer Experience**

  Customer-facing networks likewise benefit from network optimization, with faster, more available services. When customers enjoy full functionality without having to wait longer than expected, they are more likely to want to continue doing business with your company.

- **Greater Overall Network Performance**

  Obviously, the overall goal of network optimization is to optimize your network’s operation. This means better performance across the board and improved returns from any and all services and systems that rely on network performance.

8. Network Monitoring and Management :-

Network monitoring systems include software and hardware tools that can track various aspects of a network and its operation, such as traffic, bandwidth utilization, and uptime. These systems can detect devices and other elements that comprise or touch the network, as well as provide status updates.

Network administrators rely on network monitoring systems to help them quickly detect device or connection failures or issues such as traffic bottlenecks that limit data flow. These systems can alert administrators to issues via email or text and deliver reports via network analytics.

Protocols for network monitoring:-

Protocols are sets of rules and directions for devices on a network to communicate with one another. Network hardware can't transmit data without using protocols. Network monitoring systems use protocols to identify and report on network performance issues.

Key benefits of network monitoring:-

- **Clear visibility into the network**
  Through network monitoring, administrators can get a clear picture of all the connected devices in the network, see how data is moving among them, and quickly identify and correct issues that can undermine performance and lead to outages.
- **Better use of IT resources**
  The hardware and software tools in network monitoring systems reduce manual work for IT teams. That means valuable IT staff have more time to devote to critical projects for the organization.
- **Early insight into future infrastructure needs**
  Network monitoring systems can provide reports on how network components have performed over a defined period. By analyzing these reports, network administrators can anticipate when the organization may need to consider upgrading or implementing new IT infrastructure.

- **The ability to identify security threats faster**
  Network monitoring helps organizations understand what "normal" performance looks like for their networks. So, when unusual activity occurs, such as an unexplained increase in network traffic levels, it's easier for administrators to identify the issue quickly--and to determine whether it may be a security threat.

Types of network monitoring protocols:-

- **SNMP:** The Simple Network Management Protocol is an application-layer protocol that uses a call-and-response system to check statuses of many types of devices, from switches to printers. SNMP can be used to monitor system status and configuration.
- **ICMP:** Network devices, such as routers and servers, use the Internet Control Message Protocol to send IP-operations information and to generate error messages in the event of device failures.
- **Cisco Discovery Protocol:** The Cisco Discovery Protocol facilitates management of Cisco devices by discovering these devices, determining how they are configured, and allowing systems using different network-layer protocols to learn about one another.

9. Wireless Networking:-

Computer networks that are not connected by cables are called wireless networks. They generally use radio waves for communication between the network nodes. They allow devices to be connected to the network while roaming around within the network coverage.

Types of Wireless Networks:-

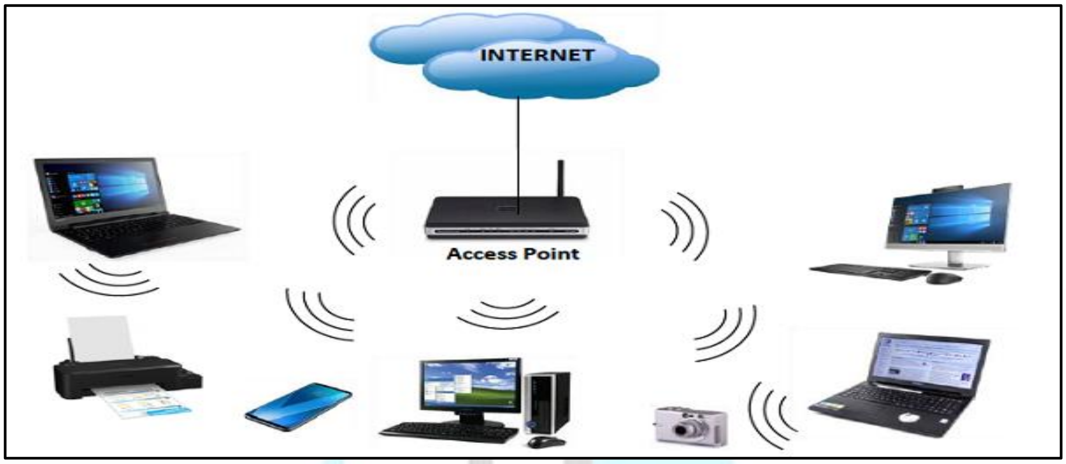
- Wireless LANs − Connects two or more network devices using wireless distribution techniques.
- Wireless MANs − Connects two or more wireless LANs spreading over a metropolitan area.
- Wireless WANs − Connects large areas comprising LANs, MANs and personal networks.

Advantages of Wireless Networks:-

- It provides clutter-free desks due to the absence of wires and cables.
- It increases the mobility of network devices connected to the system since the devices need not be connected to each other.
- Accessing network devices from any location within the network coverage or Wi-Fi hotspot becomes convenient since laying out cables is not needed.
- Installation and setup of wireless networks are easier.
- New devices can be easily connected to the existing setup since they needn’t be wired to the present equipment. Also, the number of equipment that can be added or removed to the system can vary considerably since they are not limited by the cable capacity. This makes wireless networks very scalable.
- Wireless networks require very limited or no wires. Thus, it reduces the equipment and setup costs.

Examples of wireless networks:-

1. Mobile phone networks
2. Wireless sensor networks
3. Satellite communication networks
4. Terrestrial microwave networks



In the context of the different equipments used at ***RailTel India***, some of the most common ones according to types are as follows:

➢ Routers:

- Juniper MX960 - CAPACITY 12 TBPS - Modular Card FPC Flexible PIC Concentrator, MIC Modular Interface Card, PEM Power Equipment module, SCB switching control Board, RE Routing Engine
- Juniper MX480 - CAPACITY 5.76 TBPS - Modular Card FPC Flexible PIC Concentrator, MIC Modular Interface Card, PEM Power Equipment module, SCB switching control Board
- Juniper MX240 - CAPACITY 400 GBPS
- Juniper MX104 - CAPACITY 80 GBPS
- Juniper ACX2200 - CAPACITY 60GBPS
- Cisco NCS540 - CAPACITY 420 GBPS

➢ Switches:

- Juniper EX3400
- Juniper EX3300
- Juniper EX2300
- Cisco 2960

➢ Video Surveillance Camera (in railway stations):

- DC-T3C33HRX 12MP IR 4k UHD Camera with heater.
- DC-T4236 WRX Full HD IR Bullet Camera.
- DC-D4236WRX Full HD Vandal-Resistant IR Dome Camera.
- DC-S6286HRXL-A 2MP 36x Lightmaster IR PTZ (Pan, Tilt and Zoom).

➢ <u>JUNOS software Routing Tables:</u>

The JUNOS software provides multiple routing tables that are used to manage network destinations:

- ○ inet.0
- ○ inet.1
- ○ inet.2
- ○ inet.3
- ○ inet.4
- ○ inet6.0
- ○ mpls.0
- ○ bgp.l3vpn.0
- ○ bgp.l2vpn.0

MPLS/IP Networking

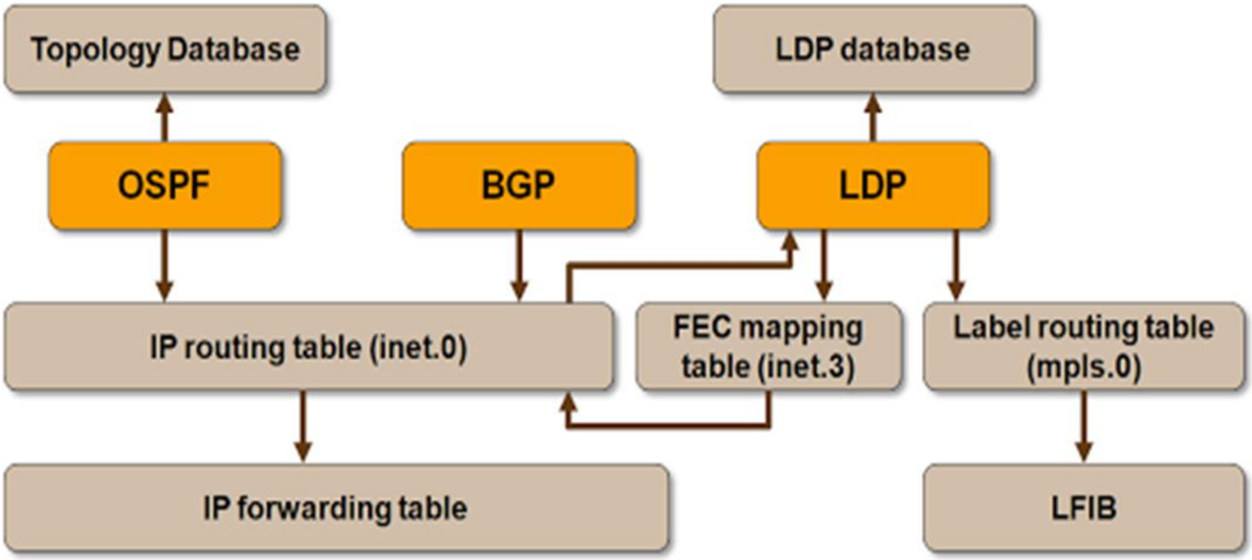
MPLS stands for Multiprotocol Label Switching. MPLS is a high-performance telecommunications technique used to speed up and manage network traffic flow. It directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table and making the data transfer process faster.

- Multi Protocol: It supports multi-protocol such as IPv4, IPv6, IPX, AppleTalk at the network layer it supports Ethernet, Token Ring, FDDI, ATM, Frame Relay, PPP at the data link layer
- Label: Labels are added to the top of the IP packet. Labels are assigned when the packet enters the MPLS domain.
- Switching: forwarding a packet based on the label value NOT on the basis of IP header information

MPLS is the integration of layer 2 and layer 3. MPLS does not replace IP; it supplements IP. QoS can be achieved through MPLS. IP and MPLS are quite similar but there are some difference between them.

IP Routing	MPLS Switching
Based on destination IP address	Based on labels
Performed at each hop of the packets path in the network	Performed only at the ingress router
Requires special multicast routing and forwarding algorithms	Requires only one forwarding algorithm

❖ MPLS Traffic Flow


Topology Database
LDP database
OSPF
BGP
LDP
IP routing table (inet.0)
FEC mapping table (inet.3)
Label routing table (mpls.0)
IP forwarding table
LFIB

- **Topology Dataset:** In MPLS, a **topology dataset** maps the network's structure, including nodes (routers, switches) and links. It helps with traffic engineering, network design, fault analysis, and performance monitoring.
- **LDP:** (Label Distribution Protocol) Dataset: An **LDP (Label Distribution Protocol) dataset** in MPLS contains information on label bindings, peer routers, label swaps, and session states. It is used to distribute and manage labels for routing data efficiently.
- **OSPF:** it stands fro Open Shortest Path First it is a link-state routing protocol used to find the best path for data through a network. It is widely used in MPLS networks to exchange routing information between routers.
- **BGP:** It stands for Border Gateway Protocol. It is a path vector routing protocol used to exchange routing information between different autonomous systems (ASes) on the internet and large networks. It is crucial for MPLS networks, particularly for inter-domain routing.
- **LDP:** It stands for Label Distribution Protocol. It is a protocol used in MPLS networks to distribute labels between routers, enabling the creation of Label Switched Paths (LSPs) for efficient data forwarding.
- **LFIB:** It stands for Label Forwarding Information Base. **It is** a data structure used by routers to make fast, efficient forwarding decisions based on labels.

❖ Advantages of MPLS:

- **Faster Data Transmission:** Uses labels for quick routing, reducing latency.
- **Efficient Bandwidth Utilization**: Traffic engineering optimizes bandwidth and prevents congestion.
- **Quality of Service (QoS):** Prioritizes critical traffic for better performance.
- **Scalability**: Handles large, complex networks efficiently.
- **Security**: Traffic isolation improves network security.
- **Cost Efficiency**: Reduces reliance on expensive routing equipment.

❖ Disadvantages of MPLS:

- **Complexity**: Initial setup and configuration can be complex.
- **Limited End-to-End Security**: MPLS itself does not provide end-to-end encryption; additional security measures are needed.
- **Dependence on Specific Providers**: Once an organization commits to MPLS, it often becomes reliant on a specific service provider for both the MPLS service and any required changes or upgrades. This can lead to less flexibility and higher costs in the long term.
- **Learning Curve**: Requires specialized knowledge and training for network management.

❖ Need of MPLS:

- **Improved Performance:** Speeds up data transmission with efficient routing.
- **Reliability**: Enhances network reliability with fast reroute and fault tolerance.
- **Flexible Path Selection**: Allows dynamic routing and rerouting of traffic.
- **Simplified Network Management**: Centralized control and management of network traffic.

RailTel VSS Network Operation

RailTel, a government-owned entity, operates a Video Surveillance System (VSS) across Indian Railways stations to enhance safety and security. This network operation involves the following key aspects:

1. **CCTV Surveillance**: RailTel installs high-definition IP-based CCTV cameras at railway stations, platforms, foot overbridges, and waiting areas. These cameras are equipped with night vision capabilities and can capture detailed footage 24/7.
2. **Centralized Monitoring**: The footage from these cameras is transmitted in real-time to a centralized control room. This allows for continuous monitoring of station premises, enabling quick response to any suspicious activities or security breaches.
3. **Network Infrastructure**: The VSS network is supported by RailTel's extensive optical fiber network, ensuring high-speed data transmission and reliable connectivity. MPLS (Multiprotocol Label Switching) is likely used for routing the video data efficiently across the network.
4. **Storage and Retrieval**: The video footage is stored in data centers and can be retrieved when needed for investigative purposes. The storage system is robust, with high-capacity servers to handle the vast amounts of data generated.
5. **Integration with Law Enforcement**: The system can be integrated with government and law enforcement databases, enabling automated facial recognition (FRS) license plate recognition, and other analytics to enhance security.

In below tentative architecture of VSS/CCTV system at stations will be as per schematic diagram 1 & 2:

Diagram 1:

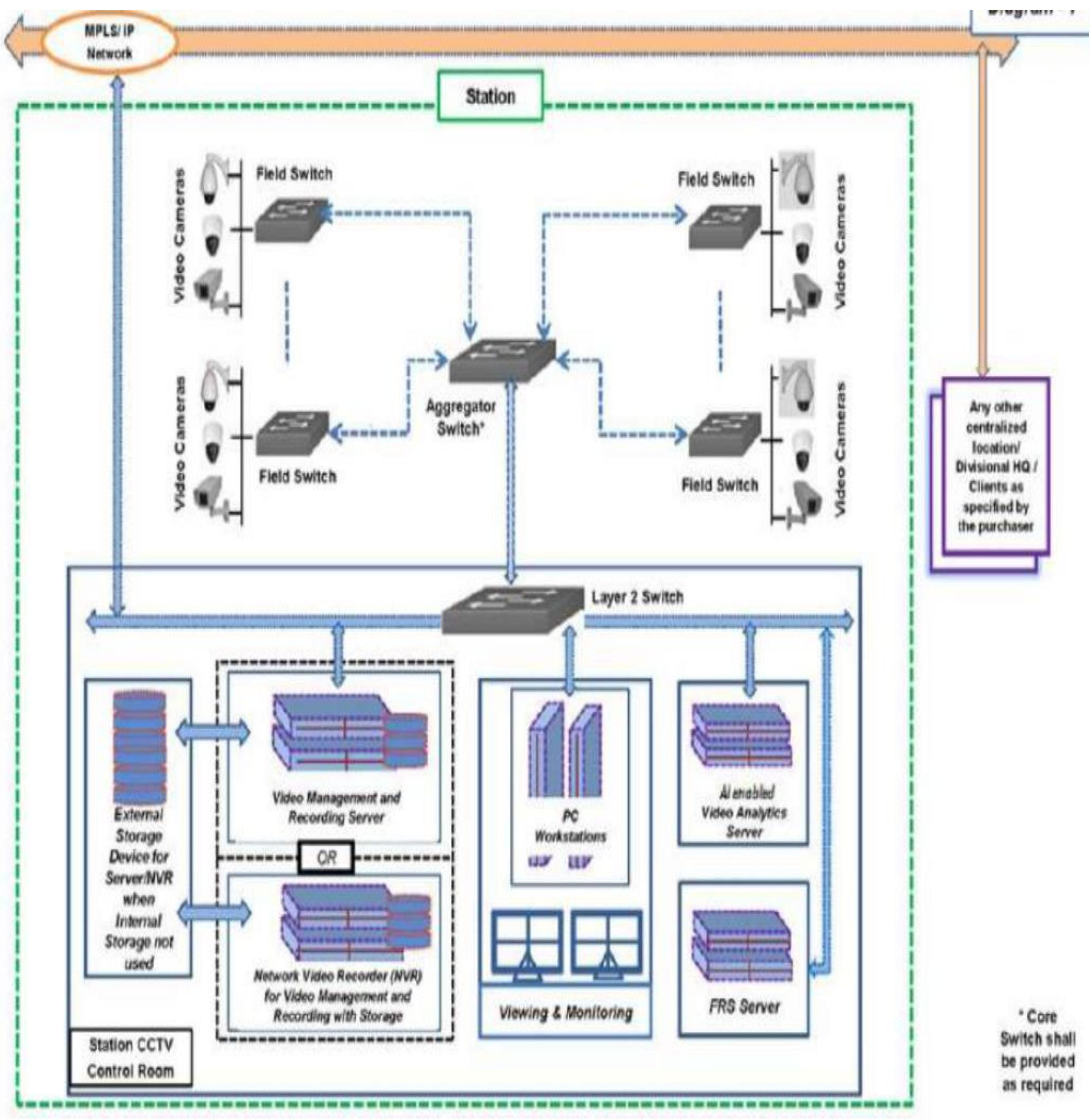
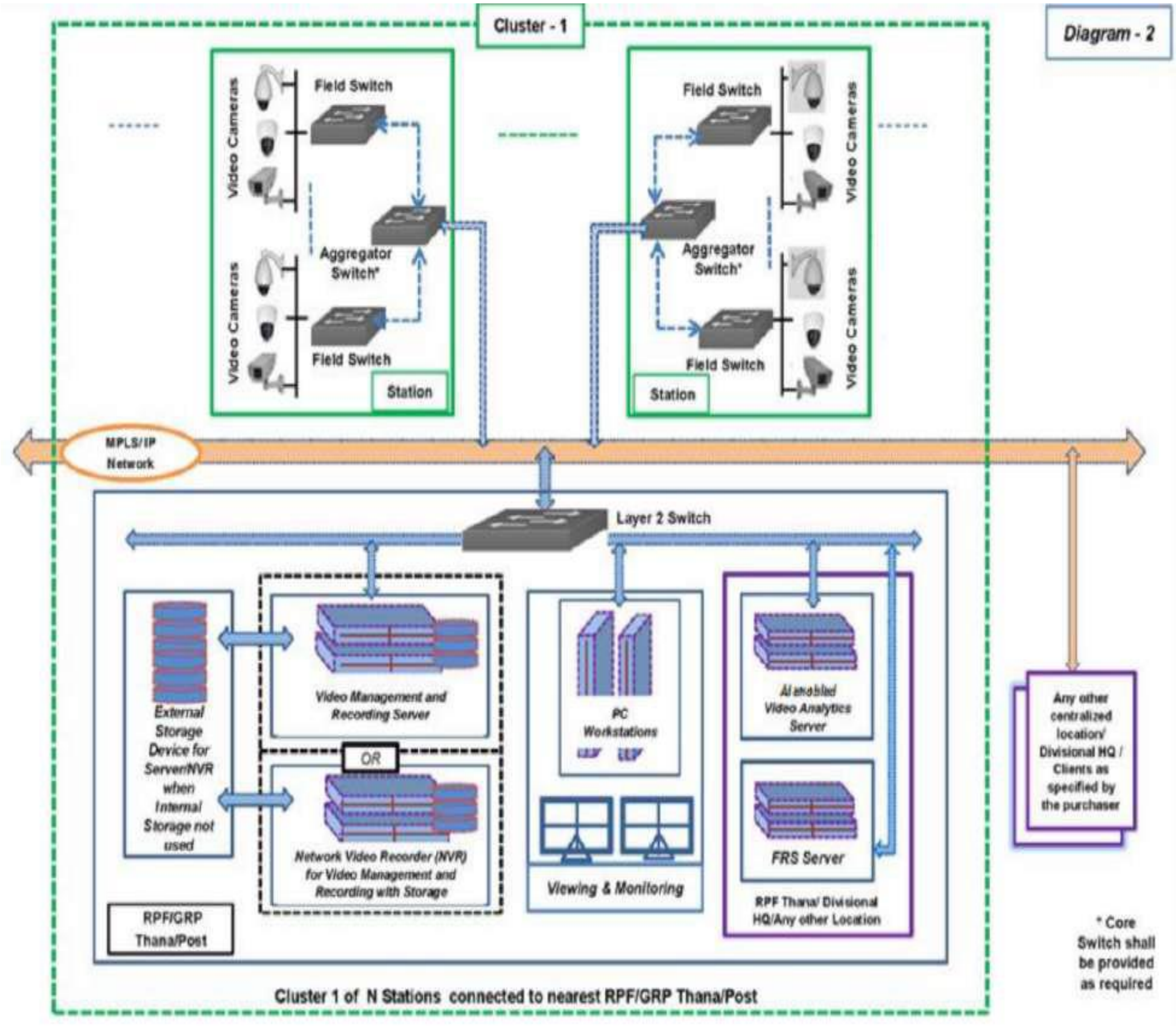


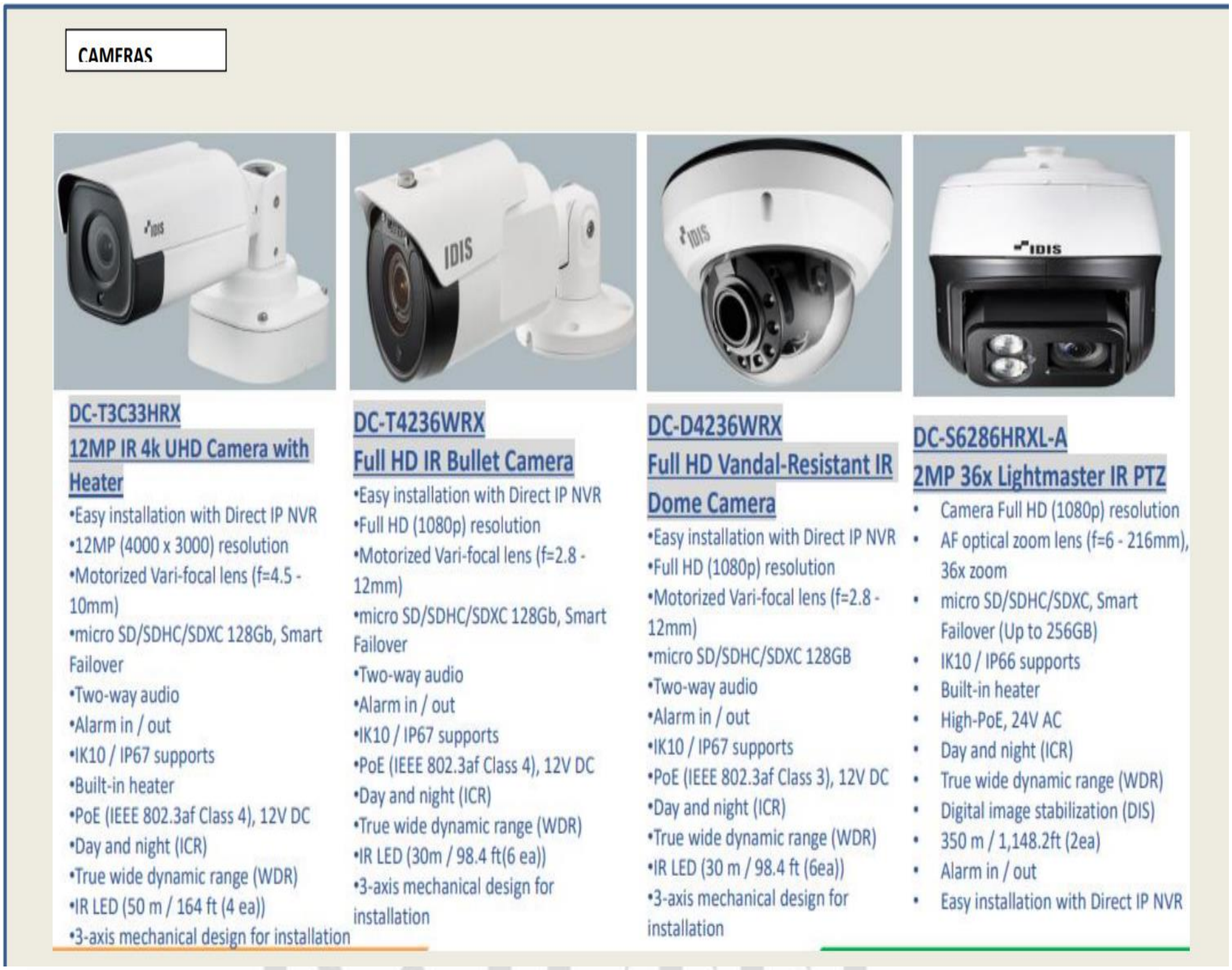
Diagram - 1
MPLS/ IP Network
Station
Video Cameras
Field Switch
Field Switch
Video Cameras
Video Cameras
Field Switch
Aggregator Switch*
Field Switch
Video Cameras
Any other centralized location/ Divisional HQ / Clients as specified by the purchaser
Layer 2 Switch
External Storage Device for Server/NVR when Internal Storage not used
Video Management and Recording Server
OR
Network Video Recorder (NVR) for Video Management and Recording with Storage
PC Workstations
Viewing & Monitoring
AI enabled Video Analytics Server
FRS Server
Station CCTV Control Room
* Core Switch shall be provided as required

Diagram 2:


Cluster - 1
Diagram - 2
Video Cameras
Field Switch
Aggregator Switch*
Video Cameras
Field Switch
Station
Field Switch
Video Cameras
Aggregator Switch*
Video Cameras
Field Switch
Station
MPLS/IP Network
Layer 2 Switch
External Storage Device for Server/NVR when Internal Storage not used
Video Management and Recording Server
OR
Network Video Recorder (NVR) for Video Management and Recording with Storage
PC Workstations
Viewing & Monitoring
AI enabled Video Analytics Server
FRS Server
RPF Thana/ Divisional HQ/Any other Location
Any other centralized location/ Divisional HQ / Clients as specified by the purchaser
RPF/GRP Thana/Post
* Core Switch shall be provided as required
Cluster 1 of N Stations connected to nearest RPF/GRP Thana/Post

Generally there are 4 types of camera are used for VSS operation:

1. 12MP IR 4k UHD Camera with Heater
2. Full HD IR Bullet Camera
3. Full HD Vandal-Resistant IR Dome Camera
4. 2MP 36x Lightmaster IR PTZ



CAMERAS

DC-T3C33HRX
12MP IR 4k UHD Camera with Heater

- Easy installation with Direct IP NVR
- 12MP (4000 x 3000) resolution
- Motorized Vari-focal lens (f=4.5 - 10mm)
- micro SD/SDHC/SDXC 128Gb, Smart Failover
- Two-way audio
- Alarm in / out
- IK10 / IP67 supports
- Built-in heater
- PoE (IEEE 802.3af Class 4), 12V DC
- Day and night (ICR)
- True wide dynamic range (WDR)
- IR LED (50 m / 164 ft (4 ea))
- 3-axis mechanical design for installation

DC-T4236WRX
Full HD IR Bullet Camera

- Easy installation with Direct IP NVR
- Full HD (1080p) resolution
- Motorized Vari-focal lens (f=2.8 - 12mm)
- micro SD/SDHC/SDXC 128Gb, Smart Failover
- Two-way audio
- Alarm in / out
- IK10 / IP67 supports
- PoE (IEEE 802.3af Class 4), 12V DC
- Day and night (ICR)
- True wide dynamic range (WDR)
- IR LED (30m / 98.4 ft(6 ea))
- 3-axis mechanical design for installation

DC-D4236WRX
Full HD Vandal-Resistant IR Dome Camera

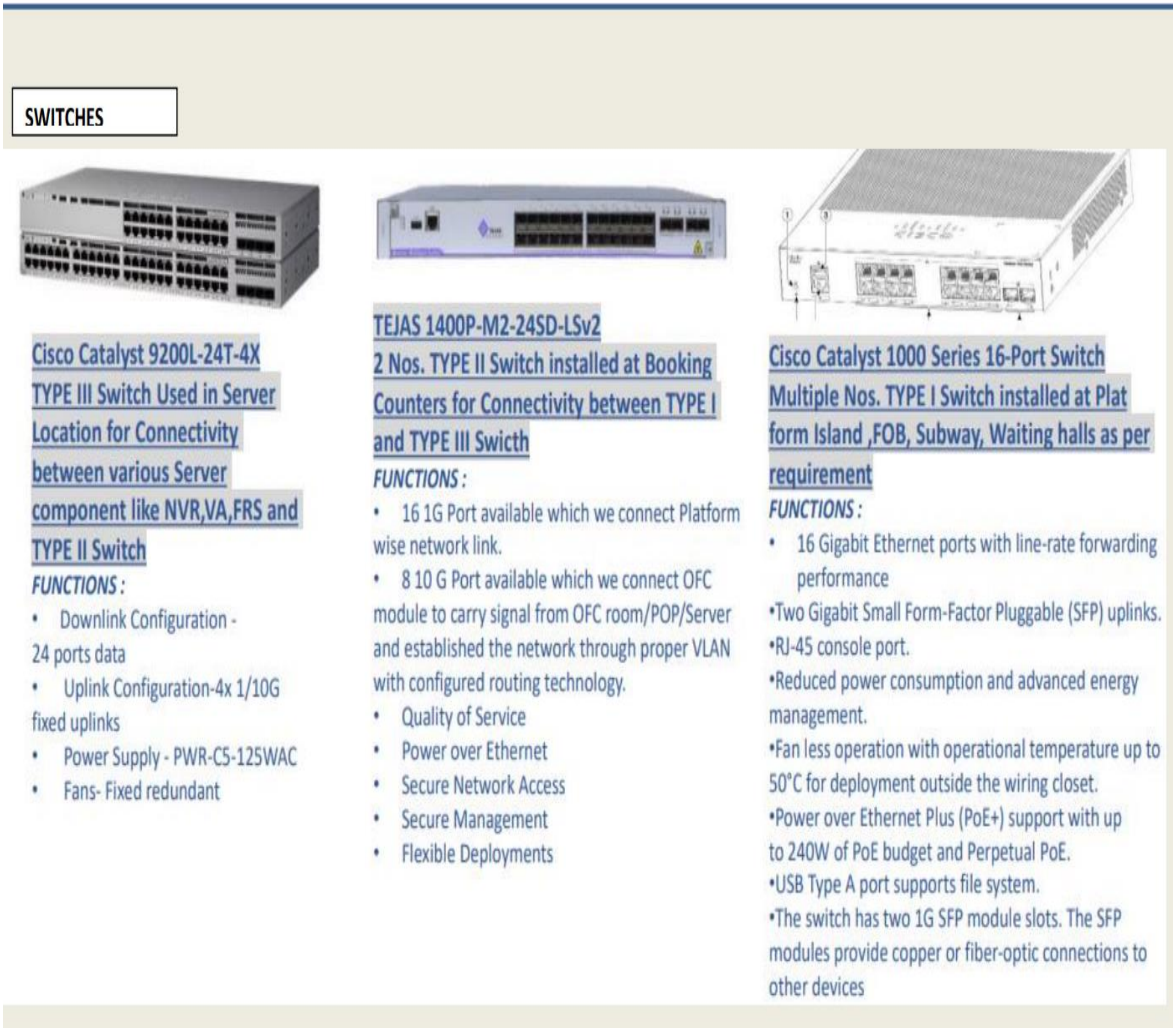
- Easy installation with Direct IP NVR
- Full HD (1080p) resolution
- Motorized Vari-focal lens (f=2.8 - 12mm)
- micro SD/SDHC/SDXC 128GB
- Two-way audio
- Alarm in / out
- IK10 / IP67 supports
- PoE (IEEE 802.3af Class 3), 12V DC
- Day and night (ICR)
- True wide dynamic range (WDR)
- IR LED (30 m / 98.4 ft (6ea))
- 3-axis mechanical design for installation

DC-S6286HRXL-A
2MP 36x Lightmaster IR PTZ

- Camera Full HD (1080p) resolution
- AF optical zoom lens (f=6 - 216mm), 36x zoom
- micro SD/SDHC/SDXC, Smart Failover (Up to 256GB)
- IK10 / IP66 supports
- Built-in heater
- High-PoE, 24V AC
- Day and night (ICR)
- True wide dynamic range (WDR)
- Digital image stabilization (DIS)
- 350 m / 1,148.2ft (2ea)
- Alarm in / out
- Easy installation with Direct IP NVR

Generally there are 3 types of switches are used for VSS operation:

1. Type-I switch
2. Type-II switch
3. Type-III switch



SWITCHES

Cisco Catalyst 9200L-24T-4X
TYPE III Switch Used in Server Location for Connectivity between various Server component like NVR,VA,FRS and TYPE II Switch

FUNCTIONS :

- Downlink Configuration - 24 ports data
- Uplink Configuration-4x 1/10G fixed uplinks
- Power Supply - PWR-C5-125WAC
- Fans- Fixed redundant

TEJAS 1400P-M2-24SD-LSv2
2 Nos. TYPE II Switch installed at Booking Counters for Connectivity between TYPE I and TYPE III Swicth

FUNCTIONS :

- 16 1G Port available which we connect Platform wise network link.
- 8 10 G Port available which we connect OFC module to carry signal from OFC room/POP/Server and established the network through proper VLAN with configured routing technology.
- Quality of Service
- Power over Ethernet
- Secure Network Access
- Secure Management
- Flexible Deployments

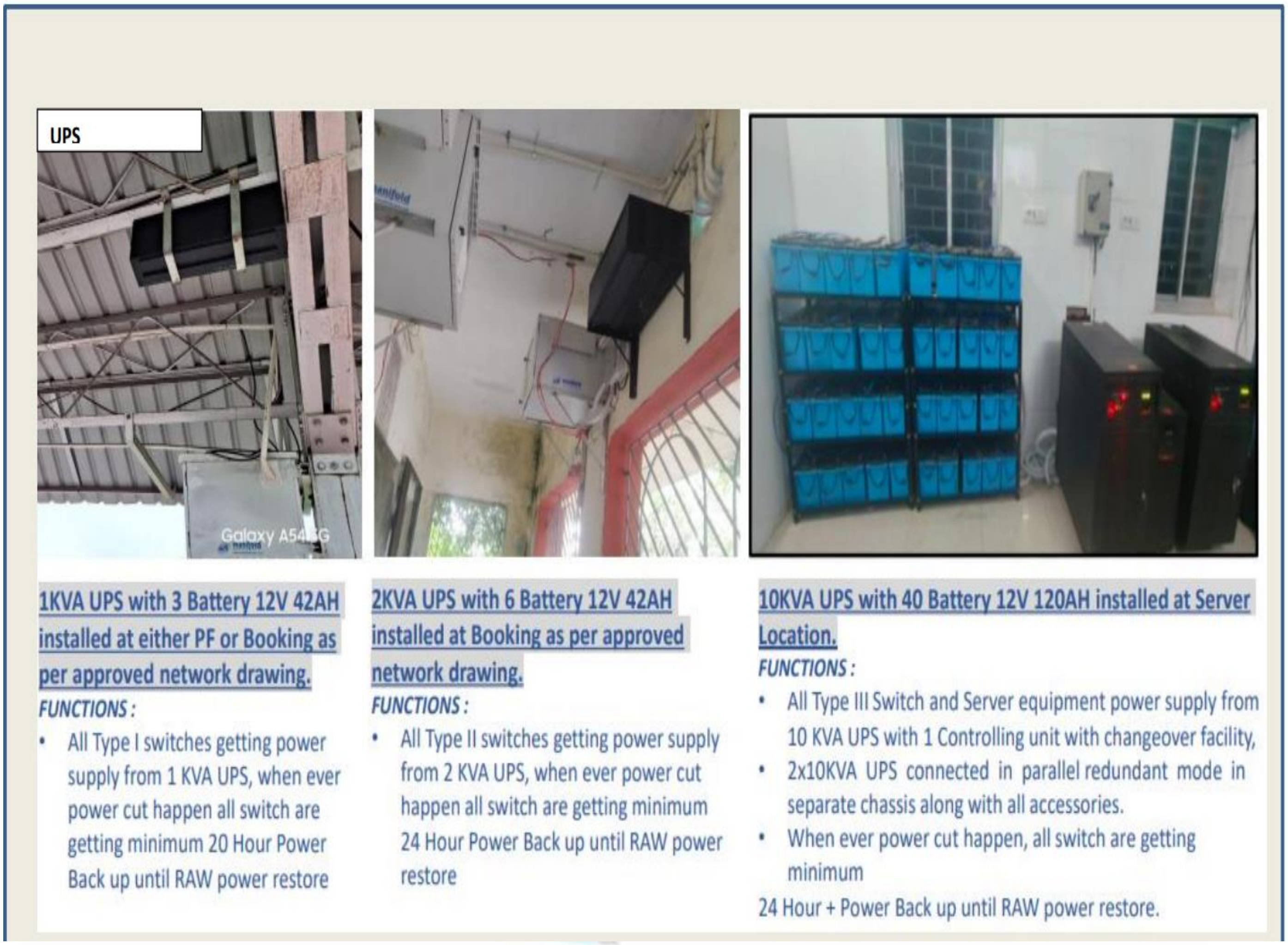
Cisco Catalyst 1000 Series 16-Port Switch
Multiple Nos. TYPE I Switch installed at Plat form Island ,FOB, Subway, Waiting halls as per requirement

FUNCTIONS :

- 16 Gigabit Ethernet ports with line-rate forwarding performance
- Two Gigabit Small Form-Factor Pluggable (SFP) uplinks.
- RJ-45 console port.
- Reduced power consumption and advanced energy management.
- Fan less operation with operational temperature up to 50°C for deployment outside the wiring closet.
- Power over Ethernet Plus (PoE+) support with up to 240W of PoE budget and Perpetual PoE.
- USB Type A port supports file system.
- The switch has two 1G SFP module slots. The SFP modules provide copper or fiber-optic connections to other devices

A UPS (Uninterruptible Power Supply) system is used in a Video Surveillance System (VSS) for several important reasons:

- **Continuous Operation**: Keeps VSS running during power outages.
- **Power Protection**: Shields equipment from power surges and fluctuations.
- **Data Integrity**: Prevents data loss or corruption.
- **Network Stability**: Maintains consistent network performance.
- **Graceful Shutdown**: Allows safe system shutdown during prolonged outages.



UPS

1KVA UPS with 3 Battery 12V 42AH installed at either PF or Booking as per approved network drawing.

FUNCTIONS :

- All Type I switches getting power supply from 1 KVA UPS, when ever power cut happen all switch are getting minimum 20 Hour Power Back up until RAW power restore

2KVA UPS with 6 Battery 12V 42AH installed at Booking as per approved network drawing.

FUNCTIONS :

- All Type II switches getting power supply from 2 KVA UPS, when ever power cut happen all switch are getting minimum 24 Hour Power Back up until RAW power restore

10KVA UPS with 40 Battery 12V 120AH installed at Server Location.

FUNCTIONS :

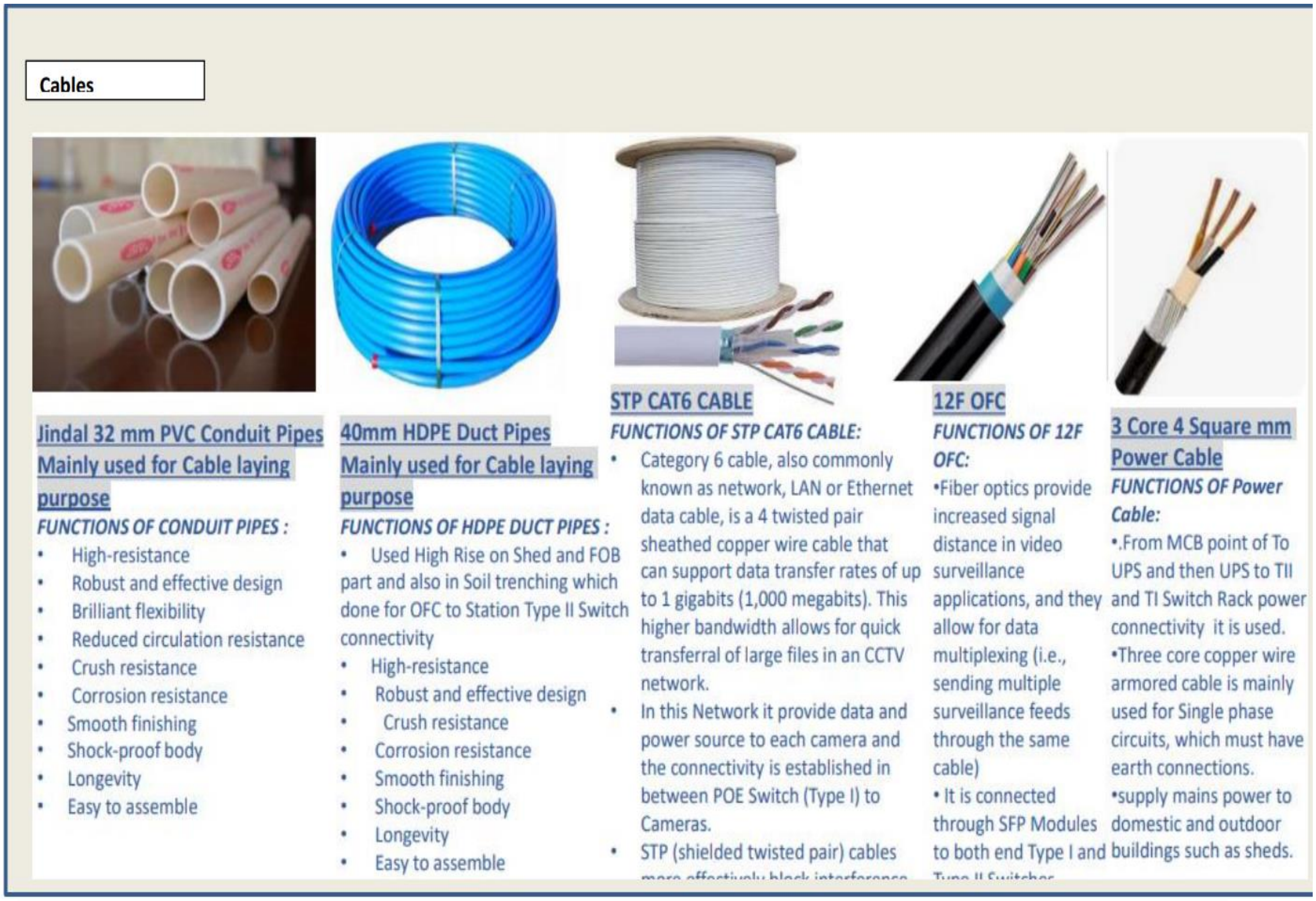
- All Type III Switch and Server equipment power supply from 10 KVA UPS with 1 Controlling unit with changeover facility,
- 2x10KVA UPS connected in parallel redundant mode in separate chassis along with all accessories.
- When ever power cut happen, all switch are getting minimum

24 Hour + Power Back up until RAW power restore.

There are also cables that are used in a Video Surveillance System (VSS) for the following reasons:

1. **Power Delivery**: Cables, especially Power over Ethernet (PoE) cables, provide power to IP cameras and other equipment, eliminating the need for separate power sources.
2. **Data Transmission**: Cables transmit video data from cameras to recording devices, network switches, and monitoring stations. Ethernet cables (like Cat5e or Cat6) are commonly used for this purpose.
3. **Reliability**: Wired connections are more stable and reliable than wireless alternatives, ensuring consistent video feed without interference or signal loss.

4. **High Bandwidth**: Cables support the high bandwidth required for transmitting high-definition video footage, especially in large-scale VSS networks.
5. **Security**: Wired connections are more secure than wireless, reducing the risk of data breaches or unauthorized access to the surveillance system.



Cables

Jindal 32 mm PVC Conduit Pipes Mainly used for Cable laying purpose

FUNCTIONS OF CONDUIT PIPES :

- High-resistance
- Robust and effective design
- Brilliant flexibility
- Reduced circulation resistance
- Crush resistance
- Corrosion resistance
- Smooth finishing
- Shock-proof body
- Longevity
- Easy to assemble

40mm HDPE Duct Pipes Mainly used for Cable laying purpose

FUNCTIONS OF HDPE DUCT PIPES :

- Used High Rise on Shed and FOB part and also in Soil trenching which done for OFC to Station Type II Switch connectivity
- High-resistance
- Robust and effective design
- Crush resistance
- Corrosion resistance
- Smooth finishing
- Shock-proof body
- Longevity
- Easy to assemble

STP CAT6 CABLE

FUNCTIONS OF STP CAT6 CABLE:

- Category 6 cable, also commonly known as network, LAN or Ethernet data cable, is a 4 twisted pair sheathed copper wire cable that can support data transfer rates of up to 1 gigabits (1,000 megabits). This higher bandwidth allows for quick transferral of large files in an CCTV network.
- In this Network it provide data and power source to each camera and the connectivity is established in between POE Switch (Type I) to Cameras.
- STP (shielded twisted pair) cables more effectively block interference

12F OFC

FUNCTIONS OF 12F OFC:

•Fiber optics provide increased signal distance in video surveillance applications, and they allow for data multiplexing (i.e., sending multiple surveillance feeds through the same cable)

• It is connected through SFP Modules to both end Type I and Type II Switches

3 Core 4 Square mm Power Cable

FUNCTIONS OF Power Cable:

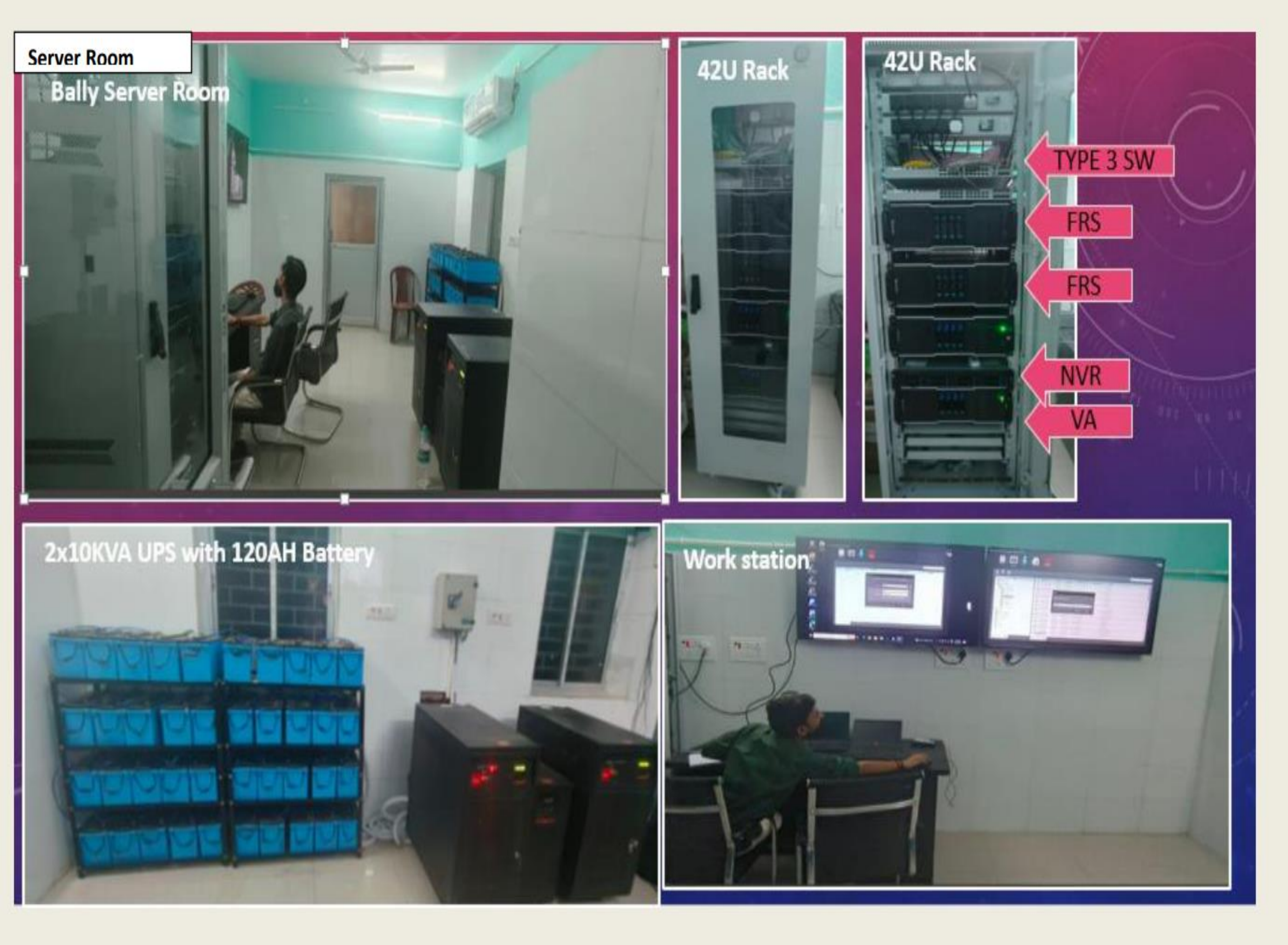
•.From MCB point of To UPS and then UPS to TII and TI Switch Rack power connectivity it is used.

•Three core copper wire armored cable is mainly used for Single phase circuits, which must have earth connections.

•supply mains power to domestic and outdoor buildings such as sheds.

There is a server room for:

1. **Centralized Data Storage**: The server room houses servers that store the vast amounts of video data captured by surveillance cameras. Centralized storage ensures easy access, management, and retrieval of footage.
2. **Processing Power**: The server room provides the necessary computing power for video processing, analytics, and management tasks, such as real-time monitoring, facial recognition, and motion detection.
3. **Network Management**: It contains network equipment like switches, routers, and firewalls, which manage the flow of data within the VSS network, ensuring efficient and secure communication.
4. **Environmental Control**: The server room is equipped with cooling systems, power backups (UPS), and fire suppression systems to maintain optimal conditions for sensitive equipment, ensuring reliable and continuous operation.
5. **Physical Security**: A dedicated server room provides physical security for critical VSS components, preventing unauthorized access and tampering with the surveillance infrastructure.



IDIS Suite Client

IDIS Solution Suite having features of recording, searching, and monitoring images from network video devices and offers the following features:

- Remote monitoring of live images

- Remote monitoring of live images in multiple Client systems through a streaming service (the number of channels that can be streamed equals the number of channels that can be recorded unless streaming WIBU-Keys have been added)

- Stable streaming by using the load balancing function in installation with more than one streaming server

- Video analytics of live images through a video analytics service

- Up to 64 simultaneous connections to the IDIS Solution Suite system

- Software upgrades and multiple systems setup remotely (supported only for devices which provide the functions)

- Display of system log information (supported only for devices which use the IDIS Solution Suite protocol)

- Map monitoring of live images

- Centralized system operation and management and event handling

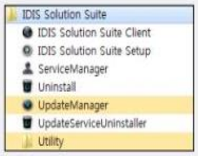
Motion Detection: Rather than continuously recording data, a VMS may also implement motion detection to reduce the amount of data to be recorded

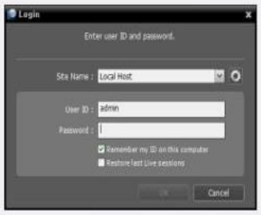
Distributed processing: The VMS provides a single management interface allowing clients to access camera sources across all servers, making them appear to be a unified collection rather than isolated on multiple independent sources.

Audio: A VMS can also be capable of recording audio from network cameras, and may in some cases provide two-way audio through a network camera, acting as an intercom which can be remotely rotated, titled and zoomed, thereby allowing a single camera to monitor a very large area while also providing detailed views of specific areas of interest.

IDIS Client Login & configuration of device & services

Go to the **Start** Menu → Click **IDIS Solution Suite** → Run the **IDIS Solution Suite Setup** or **IDIS Solution Suite Client** program and enter login information.





Login

Enter user ID and password.

Site Name : Local Host

User ID : admin

Password :

☑ Remember my ID on this computer

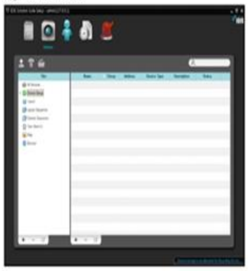
□ Restore last Live sessions

OK Cancel

Registering Devices

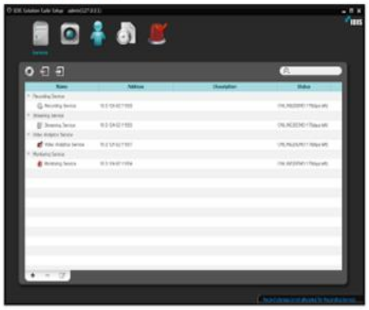
You must register devices on the administration service and add the devices to a device group in order to perform any operation.

Go to the **Start** Menu → Click **IDIS Solution Suite** → Run the **IDIS Solution Suite Setup** program and enter login information.



1 Select the **Device** menu.

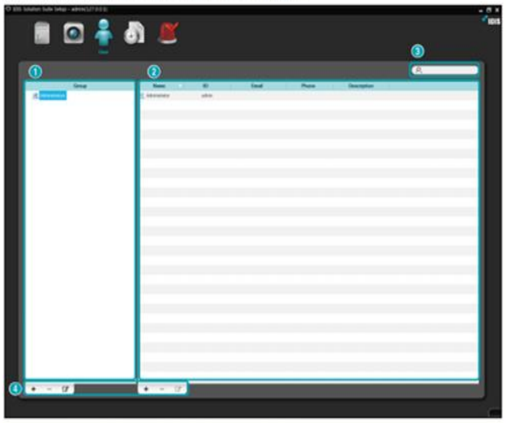
2 Select recording, monitoring, streaming and video analytics services to register on the IDIS Solution Suite system, and the selected services are displayed in the service list.



USER Management

User

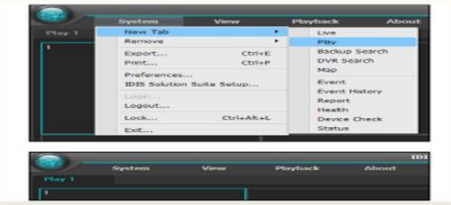
The User menu allows you to register and manage users or user groups.



1	**Group Panel**	Displays a user group list. The **Administrators** group has authority to perform all functions, and the authority settings cannot be edited.
2	**User List Panel**	Displays the list and information about users registered in each group.
3	**(Incremental Search)**	Allows you to search for a user registered in each group. Selecting a group in the **Group** Panel and entering text that you want to search for causes the search results to be displayed. Search results are displayed immediately as matching text is found within the selected group. As you enter more text, the results narrow.
4	**+ (Add),** **− (Remove),** **☐ (Edit)**	Allow you to add, remove and edit a user group or user.

Recorded Video Playback & Exportation

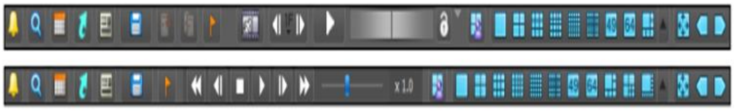
Select a site to connect to from the Site list and drag and drop it on the Play or DVR Search screen. Recorded video from the selected site is displayed on the screen. You can move a camera screen to the desired location on the Play or DVR Search screen without stopping the current playback while playing back video. Select a camera screen and drag and drop it on the desired location.

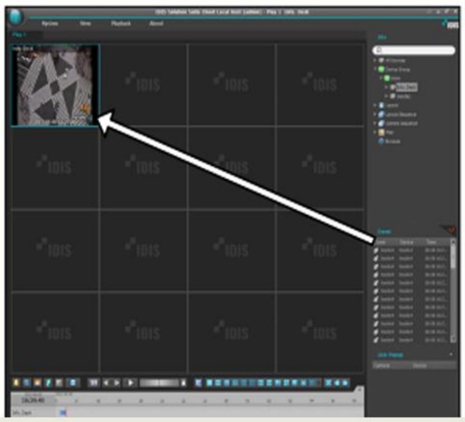


Panel Toolbar

The toolbar at the bottom of the panel allows you to search and play back recorded video.

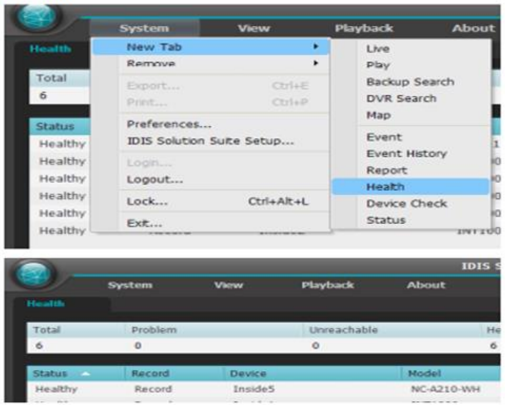
☑ The toolbar may be different and some functions below may not be supported, depending on the specifications and version of the device.



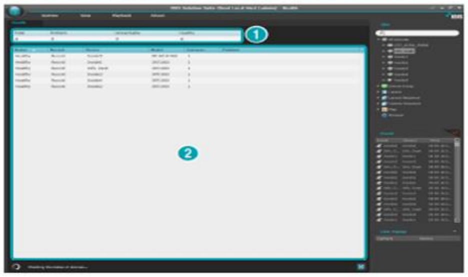


Health Monitoring

System health monitoring is supported in the Health panel (supported only for devices registered on recording services). If the Health tab is not on the tab panel, go to the **System** menu, click **New Tab** and **Health**.

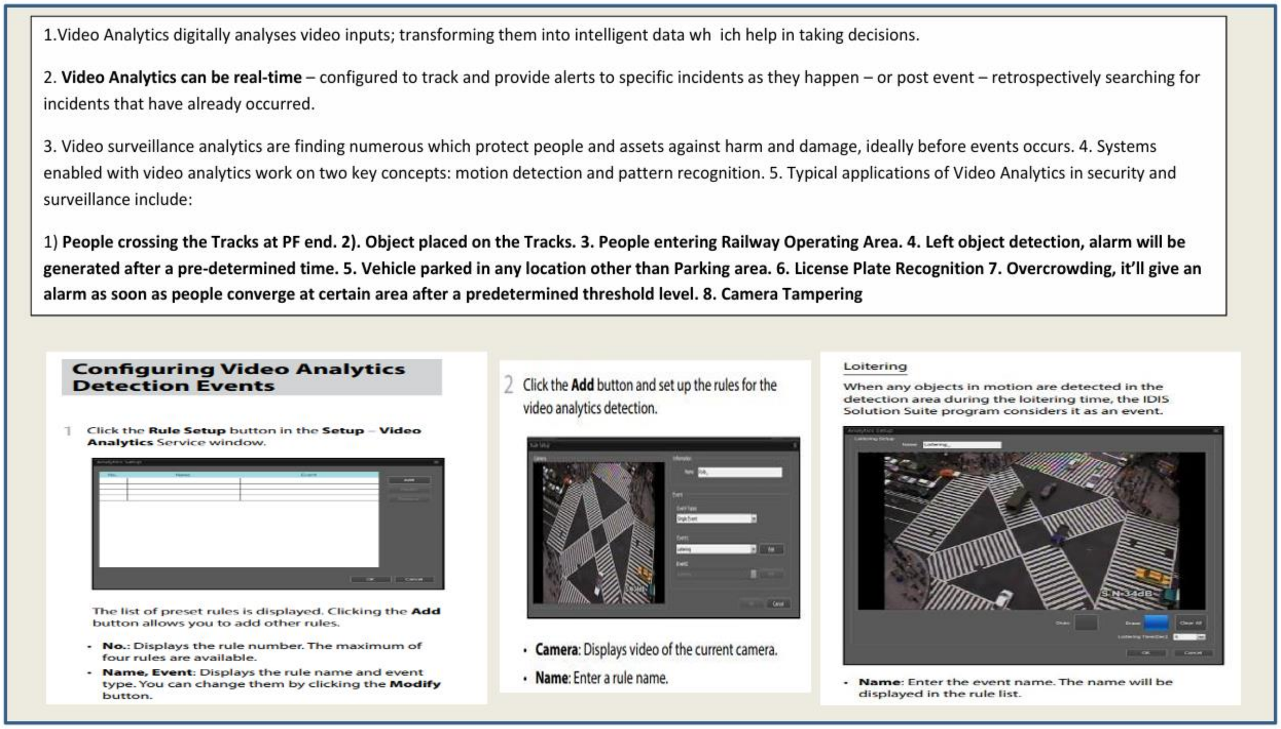


The Client program automatically displays the health monitoring results when the Health tab is added.



① **Summary List**: Displays the health monitoring status of all devices registered on recording services in summary.

- **Total**: Displays the number of devices registered on recording services.
- **Problem**: Displays the number of devices where a problem is detected.
- **Unreachable**: Displays the number of devices that are not connected.



1.Video Analytics digitally analyses video inputs; transforming them into intelligent data wh ich help in taking decisions.

2. **Video Analytics can be real-time** – configured to track and provide alerts to specific incidents as they happen – or post event – retrospectively searching for incidents that have already occurred.

3. Video surveillance analytics are finding numerous which protect people and assets against harm and damage, ideally before events occurs. 4. Systems enabled with video analytics work on two key concepts: motion detection and pattern recognition. 5. Typical applications of Video Analytics in security and surveillance include:

1) **People crossing the Tracks at PF end. 2). Object placed on the Tracks. 3. People entering Railway Operating Area. 4. Left object detection, alarm will be generated after a pre-determined time. 5. Vehicle parked in any location other than Parking area. 6. License Plate Recognition 7. Overcrowding, it'll give an alarm as soon as people converge at certain area after a predetermined threshold level. 8. Camera Tampering**

Configuring Video Analytics Detection Events

1 Click the **Rule Setup** button in the **Setup** – **Video Analytics** Service window.

The list of preset rules is displayed. Clicking the **Add** button allows you to add other rules.

- **No.**: Displays the rule number. The maximum of four rules are available.
- **Name, Event**: Displays the rule name and event type. You can change them by clicking the **Modify** button.

2 Click the **Add** button and set up the rules for the video analytics detection.

- **Camera**: Displays video of the current camera.
- **Name**: Enter a rule name.

Loitering

When any objects in motion are detected in the detection area during the loitering time, the IDIS Solution Suite program considers it as an event.

- **Name**: Enter the event name. The name will be displayed in the rule list.

In conclusion, Cisco's Virtual Switching System (VSS) offers several significant advantages for modern network infrastructures:

- Enhanced Redundancy: VSS provides high availability by allowing one switch to take over if another fails, minimizing network downtime.
- Simplified Management: By consolidating multiple switches into a single virtual switch, VSS reduces the complexity of network management.
- Improved Bandwidth Utilization: VSS eliminates the need for Spanning Tree Protocol (STP), effectively doubling the available bandwidth.
- Increased Network Reliability: The system ensures continuous synchronization between switches, enhancing fault tolerance.
- Operational Efficiency: VSS streamlines network operations, reducing the time and cost associated with managing multiple switches.
- These benefits make VSS a powerful tool for organizations looking to optimize their network performance and reliability.

Thank You