➢ **EQUIPMENTS:**

- Core Switch
- Distribution Switches
- Router
- Fiber Optic Cables
- Ethernet Cables
- Modems
- Access Points
- Firewall
- Patch Panels
- Power Over Ethernet (PoE) Switches
- Network Racks
- Uninterruptible Power Supply (UPS)
- Fiber Optic Transceivers
- Network Interface Cards (NICs)
- Cable Management Tools
- Crimping Tools
- Cable Testers
- Antennas (for point-to-point links)
- Grounding Equipment

➢ Check Network Infrastructure:

- **Topology Choice:** Select an efficient topology, like star or partial mesh, to connect 1200 users across a 2 km area.
- **Equipment Selection:** Choose reliable networking devices such as switches and routers for seamless connectivity.
- **Internet Connectivity:** Establish partnerships with upstream ISPs or connect to exchange points for internet access.
- **Security Measures:** Implement robust security protocols, including firewalls and intrusion detection systems, to protect the network.
- **Scalability and Compliance:** Plan for scalability and comply with local regulations, ensuring sustainable growth and legal operation as an ISP.

➢ Set Up Backbone Infrastructure:

Setting up the backbone infrastructure involves:

Installing Core Devices:

Deploy routers and switches as central networking devices

Connecting Devices:

Use appropriate cables to interconnect routers and switches securely.

Enable Port Security:

Limit the number of devices that can connect to each switch port.
Enhances network security by preventing unauthorized devices.

Implementing Redundancy:

Establish redundancy protocols like **Virtual Router Redundancy Protocol (VRRP)** or HSRP for high availability.

➢ Set Up Routing and Switching:

Configure routing and switching equipment.

Router:

Use a high quality of the router to manage network traffic and ensure efficient data flow

Consider a router with advance features like quality of server(QOS) for Bandwidth management

Here are some reputable router manufacturers and series that are commonly used in ISP environments:

- **Cisco ISR Series**
- **Juniper MX Series**
- **TENDA-F3**
- **HPE Aruba 5400R Series**

HuB/Switch:

Use hub/switch as a central device which employ ethernet switches to connect within the local network .switches offer more control over the network traffic .

Here are some examples of switch that are commonly used in Local area networks :

- **Cisco Catalyst Series:**

  Cisco Catalyst switches are popular for their reliability.

  Catalyst 2960-X or 3850 series are common choices for access and distribution layers.

- **HPE Aruba 2930F:**

  Aruba switches provide a robust feature set and are easy to manage.

  Aruba 2930F series is suitable for various network sizes.

- **Dell EMC PowerSwitch:**

  Dell PowerSwitch switches offer flexibility and scalability.

  Models like Dell EMC PowerSwitch 5400 series are suitable for enterprise networks.

➢ Set Up DHCP and DNS Services:

DHCP (Dynamic Host Configuration Protocol):

ISC DHCP Server:
Widely used open-source DHCP server.
Offers flexibility and is feature-rich.
Suitable for small to large networks.
Microsoft DHCP Server:
Integrated with Windows Server.
Ideal for Windows-centric environments.
Supports dynamic IP address assignment.
Cisco DHCP Server:
Available on Cisco routers and switches.
Convenient for integrated DHCP services.
Common in Cisco-centric network setups.

Reasons:

Compatibility
Ease of Integration
Features and Flexibility

DNS (Domain Name System):

Microsoft DNS Server:

Integrated with Windows Server.
Seamless integration with Active Directory.
Common choice in Windows-centric environments.

Google Cloud DNS:

Cloud-based DNS service.
Offers global coverage and scalability.
Suitable for cloud-centric or distributed setups.

Reasons:

Integration: Choose DNS services that integrate well with your existing infrastructure.
Scalability: Consider the scalability of DNS servers, especially for growing networks or cloud-based services.
Support for Features: Ensure that the DNS server supports features like DNSSEC, caching, and logging, based on your requirements.

➢ Set Up NAT (Network Address Translation):

Cisco IOS NAT:

Integrated into Cisco routers and switches.
Provides dynamic and static NAT configurations.
Commonly used in Cisco-centric network setups.

pfSense NAT:

Open-source firewall and routing software.
Offers NAT functionality in addition to firewall capabilities.
Suitable for small to medium-sized networks.

Microsoft Forefront Threat Management Gateway (TMG):

Legacy Microsoft product, still used in some environments.
Combines firewall, VPN, and NAT functionalities.
Integrated with Windows Server.

Reasons:

Device Compatibility: Choose NAT solutions compatible with your network devices.
Integration with Other Services: Consider solutions that integrate well with your existing network services.
Ease of Configuration: Choose NAT solutions that align with your level of expertise and configuration requirements.

➢ Set Up Customer Connections:

Modem:

Provides the initial link between the customer premises and the ISP network.
Converts digital signals from the ISP to analog signals for transmission over the customer's line.

Cabling (Ethernet, Fiber, etc.):

Use appropriate cables to connect the customer's equipment to the ISP's network.
Ethernet cables are common for wired connections.

For example:

Category 6a (Cat6a):

Improved performance and bandwidth compared to Cat6.
Supports speeds up to 10 Gbps at longer distances.
Suitable for high-performance data centers and enterprise networks.

Set Up Hybrid topology:

Given the requirement of providing a wired network to 1200 users in a 2 km local area, a **Hybrid Topology** would likely be more suitable.

Star Topology for User Clusters:

- Implement a star topology for individual user clusters or buildings within the 2 km area.
- Use a central switch or router in each cluster to connect individual devices.

Point-to-Point (P2P) Links for Longer Distances:

- For longer-distance connections between clusters or critical locations, consider point-to-point links.
- Use high-capacity directional antennas or fiber optics for reliable and high-speed connections.

Partial Mesh-topology for Redundancy:

- Establish direct links between critical locations, forming a partial mesh.
- Prioritize redundancy for high-traffic or mission-critical areas.

Monitoring Network Performance and Security:

- **Network Monitoring Tools:** Identify performance issues, bandwidth usage, and potential bottlenecks.
- **IDS/IPS:** Detect and prevent unauthorized access, attacks, or suspicious activities.
- **Firewall Logs:** Analyze firewall logs to understand traffic patterns and detect anomalies.
- **SIEM Systems:** Centralize and correlate log data for comprehensive security analysis.
- **Packet Capture Tools:** Capture and analyze network packets for troubleshooting and forensic Analysis

➢ CONCLUSION:

In conclusion, establishing a wired network as a local ISP involves deploying a strategic combination of topologies like star or partial mesh, selecting suitable networking equipment, and connecting to upstream providers or exchange points for internet access. Careful planning of network architecture, security measures, and scalability is crucial to ensure reliable service for the 1200 users across a 2 km area. Building strong partnerships with upstream ISPs or exchange points, along with adherence to local regulations, will contribute to the success and sustainability of the ISP venture.

THE END