Power System Protection and Control
ISSN:1674-3415

A CIDR ROUTING TECHNIQUE FOR PATIENT REAL TIME DIAGNOSIS WITH MILLION SQUARE ROUTING

Binu C T, Rubini P

SOET, CMR University,Bengaluru

Received: 15/11/2025 **Revised**: 22/12/2025 **Accepted**: 08/01/2026

***ABSTRACT*:**

It is essential that real time medical diagnosis need a Classless Inter-Domain Routing. The CIDR routing with masking helps to dynamically locate the patient with help of Urgent data. Urgent data in CIDR transfer and receive with the help of automatically adjusting IP prefixes and routing tables. It the fastest routing technique for patients and hospitals. Million square routing is a proposed routing technique helps to monitor patients. In million square two IP one for hospital and one for patient. Each patient have unique IP in the hospital to connect. Its faster and secure VPN. The cloud environment with multiple hospital need this routing for rapid connection and it has low response time

INTRODUCTION

CIDR, or Classless Inter-Domain Routing, is a method used in networking to allocate IP addresses more efficiently than the older class-based system (Class A, B, C). Introduced in 1993, CIDR allows for flexible subnetting by using a suffix called a *prefix length* (e.g., /24) to indicate how many bits of the IP address represent the network portion. This flexibility helps reduce the waste of IP addresses that occurred with fixed classes, allowing organizations to use only the number of addresses they actually need.

CIDR works by representing IP addresses and their subnet masks in a compact format. For example, the CIDR notation 192.168.1.0/24 means that the first 24 bits of the address define the network, leaving the remaining 8 bits for host addresses within that network. This method enables the creation of subnets of varying sizes, unlike the rigid classes of the past. It also allows multiple smaller networks to be aggregated into a single routing entry, reducing the size of routing tables and improving the efficiency of data transmission across the internet. The main benefits of CIDR include efficient IP address utilization and simplified routing. By allowing variable-length subnet masks, networks can avoid the waste of large address blocks and make better use of available addresses. CIDR also supports route aggregation, which reduces the complexity and size of routing tables in large networks, making internet routing faster and more scalable. Overall, CIDR has been a critical development in modern networking, helping the internet expand while conserving limited IPv4 address space

LITERATURE SURVEY

Limitations of class-based addressing.

- CIDR addresses IPv4 address exhaustion and explosive growth of routing tables by replacing fixed class A/B/C blocks with variable-length prefixes.
- It proposes topological allocation of IP space and aggregation rules to slow routing table growth.
  RFC 1518 — *An Architecture for IP Address Allocation with CIDR*
- Defines the architecture and technical plan for address allocation using CIDR, focusing on how to manage IP assignments and routing domains efficiently.

RFC 4632 — *Best Current Practice for CIDR*

- Updates and clarifies the original RFC 1519 strategy with lessons from deployment over more than a decade.
- Discusses conserved address space, CIDR implementation, and routing considerations in modern Internet infrastructure.

2. Core Academic and Technical Papers

CIDR Mechanism and Scaling

DOI: 10.46121/pspc.54.1.2

"CLASSLESS INTER DOMAIN ROUTING – CIDR" (Luoma, 1996)

- A detailed academic report showing how CIDR eliminates rigid class boundaries, uses arbitrary IP prefixes, and supports route aggregation to combat routing table explosion.
- It explores efficient address allocation and how CIDR impacts inter-domain advertisement.
  ResearchGate Paper on CIDR Deployment and Strategy
- Discusses the CIDR prefix allocation strategy and its long-term effects on global routing state.
- Provides retrospective analysis on address assignment policies after years of CIDR use.

3. Related Research Topics Influenced by CIDR

Routing and Address Lookup Complexity

IP Address Lookup Algorithms (IIT Bombay Survey)

- CIDR's flexible prefixes improve address utilization but require longest prefix match (LPM) lookups, which complicate traditional exact match routing.
- This survey examines how CIDR affects routing table search algorithms and scalability.
  Distributed Route Aggregation (ACM Paper)
- Focuses on aggregation techniques influenced by CIDR's principles, presenting ways to group prefixes to reduce global routing entries.
- Addresses fundamental issues in forwarding table optimization for large networks.

4. Secondary Sources and Tutorials

General Networking Overviews

- CIDR is now the Internet backbone's standard approach for IP allocation and routing, supported by major protocols like BGP. It enables aggregate routing and reduces routing table size significantly compared to classful addressing.
- CIDR eliminated rigid blocks (Class A/B/C), promoting precise allocation based on need, and introduced the current slash notation (/n) to indicate prefix length.
  Comparative and Practical Discussions
- Other articles discuss the trade-offs of CIDR (complexity and planning overhead vs. address efficiency and routing table reduction).

5. Key Themes in Literature

CIDR's Motivation

- *IPv4 address scarcity:* CIDR allows variable-sized blocks matching organizational needs, reducing wasted addresses.
- *Routing table growth:* Route aggregation under CIDR limits the number of individual entries advertised across the Internet. r
  CIDR Operations
- Aggregation (Supernetting): combining contiguous address blocks into a single prefix.
- Longest Prefix Match (LPM): algorithmic necessity introduced by CIDR due to variable prefix lengths.

- Implementation and Challenges
  Protocol Changes: Routing protocols like BGP were updated to carry prefix length information instead of assuming fixed class sizes. r
- *Lookup Complexity:* CIDR complicates routing lookup mechanisms, motivating research into faster LPM structures
  Evolution and Integration
- CIDR's strategies were integrated into IPv6 deployment to further conserve address space and improve scalability.

6. Suggested Reading List (for deeper study)

1. RFC 1519 / RFC 4632 – Core CIDR standards and best current practices
2. Marko Luoma's CIDR survey – Academic overview with technical insights
3. Route Aggregation papers – Explore scalability implications in routing infrastructure.
4. IP Lookup Algorithms Survey – Understand algorithmic effects of CIDR.

📌 **Summary for Literature Survey**

DOI: 10.46121/pspc.54.1.2

- CIDR evolved from early IP addressing problems and was standardized by IETF in the early 1990s to optimize address space and curb routing table growth
- Core RFCs lay out both address allocation frameworks and routing aggregation techniques.
- Research builds on these by focusing on aggregation mechanisms, lookup optimization, and scaling strategies in modern networks involves automatically adjusting IP prefixes and routing tables when:
- Networks grow or shrink
- Links go up/down
- Traffic patterns change

Typical steps to dynamically reconfigure CIDR routes

1. Enable a classless routing protocol

Enabling a classless routing protocol means configuring a network device, like a router, to support routing methods that do not rely on fixed IP address classes (A, B, or C) and can handle variable-length subnet masks (VLSM). Classless protocols, such as OSPF, EIGRP, or RIP version 2, include the subnet mask information in routing updates, allowing routers to make more precise forwarding decisions and efficiently use IP address space. This is important for modern networks because it allows for flexible subnetting, reduces wasted addresses, and supports route aggregation, which helps keep routing tables smaller and improves network performance. By enabling a classless protocol, networks can scale more effectively and adapt to complex addressing schemes without being limited by traditional class boundaries.

2. Advertise CIDR prefixes

Advertising CIDR prefixes means that a router shares network routes using Classless Inter-Domain Routing (CIDR) notation in its routing updates, including both the network address and its prefix length (e.g., 192.168.1.0/24). This allows other routers in the network to understand the exact size of the subnet and route traffic efficiently. By advertising CIDR prefixes, networks can use variable-length subnet masks (VLSM), reduce wasted IP addresses, and support route aggregation, which combines multiple smaller networks into a single routing entry. This practice improves scalability, reduces the size of routing tables, and ensures that routing decisions are accurate and optimized for modern, flexible network designs

3. Allow automatic route updates

Allowing automatic route updates means configuring a router to dynamically share and receive routing information with other routers in the network without manually entering each route. This is typically done using dynamic routing protocols like RIP, OSPF, or EIGRP, which automatically detect network changes and update routing tables in real time. By enabling automatic updates, routers can quickly adapt to new networks, failed links, or topology changes, ensuring that data always takes the most efficient path. This reduces administrative work, minimizes routing errors, and helps maintain a more reliable and scalable network.

4. Apply summarization where needes

Applying summarization in networking means combining multiple specific routes into a single, broader route before advertising them to other routers. This technique, often called route summarization or supernetting, helps reduce the size of routing tables, decreases network overhead, and simplifies routing decisions. For example, instead of sending individual routes for 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24, a router can advertise them as a single summarized route, 192.168.0.0/22. Using summarization where needed improves network efficiency, speeds up routing, and prevents unnecessary complexity in large networks.

5. Monitor convergence

Monitoring convergence in CIDR-based networks involves tracking how quickly routers update their routing tables after a change in the network, such as a link failure or addition of a new subnet. Because CIDR allows for classless routing and variable-length subnet masks, convergence ensures that all routers have the correct network information, including the proper CIDR prefixes. Network administrators monitor convergence to confirm that routes are propagated accurately and efficiently, minimizing downtime or routing loops. Fast and stable convergence is essential for maintaining reliable communication across the network and ensuring that traffic always takes the most efficient path.

Role of CIDR in Online Medical Assessment Platforms

Online medical assessment systems (used for tests, diagnostics, or remote evaluations) rely heavily on secure, scalable, and reliable networks. CIDR helps support these needs in several ways:

DOI: 10.46121/pspc.54.1.2

1. Efficient Network Management

Efficient network management in CIDR involves using classless addressing and variable-length subnet masks (VLSM) to optimize the allocation and use of IP addresses across a network. By organizing networks with precise CIDR prefixes, administrators can avoid wasting address space, simplify routing, and reduce the size of routing tables through techniques like route summarization. This makes it easier to plan, monitor, and troubleshoot networks, especially large or growing ones, while ensuring scalability and better performance. Overall, CIDR enables more flexible, organized, and cost-effective network management compared to traditional class-based addressing.

- CIDR allows hospitals, clinics, and assessment platforms to allocate IP addresses based on actual need.
- This avoids wasting IP addresses and supports scalability as more users (patients, doctors, students) join the system.

2. Improved Security

Improved security in CIDR comes from its ability to control and limit the scope of network traffic using precise subnetting and routing. By dividing a network into smaller, well-defined CIDR-based subnets, administrators can isolate sensitive systems, enforce access rules, and reduce exposure to potential attacks. Combined with firewall policies and route filtering, CIDR allows networks to restrict which subnets can communicate with each other, making unauthorized access more difficult. This precise control over IP address allocation and routing not only enhances security but also helps detect and contain network threats more effectively.

- CIDR-based subnetting helps isolate sensitive medical assessment servers from public networks.
- Only specific IP ranges can be allowed access, reducing unauthorized entry and protecting patient data.

3. Better Performance and Reliability

Better performance and reliability in CIDR come from its ability to organize networks efficiently using classless addressing and variable-length subnet masks (VLSM). By allocating IP addresses precisely and using techniques like route summarization, CIDR reduces the size of routing tables and minimizes unnecessary network traffic. This leads to faster routing decisions, less congestion, and lower latency across the network. Additionally, CIDR's support for flexible subnetting and quick route updates helps maintain stable connectivity even when parts of the network fail, improving overall reliability and ensuring consistent performance for users and applications.

- CIDR reduces the size of routing tables, making data transmission faster and more efficient.
- This is important for real-time assessments such as online exams, telemedicine evaluations, or diagnostic uploads.

4. Access Control for Assessments

Access control for assessments in CIDR involves restricting or permitting network access based on IP address ranges defined by CIDR prefixes. By using precise subnetting, administrators can control which devices or users can reach certain resources, such as online tests, lab environments, or assessment servers. This ensures that only authorized users from specific subnets can participate, while others are blocked, enhancing security and integrity. Implementing CIDR-based access control also makes it easier to manage large networks, enforce policies consistently, and prevent unauthorized access during critical assessments or educational activities.

- Medical assessments can be restricted to specific IP ranges (e.g., hospital networks or exam centers).
- CIDR makes it easy to define and manage these trusted IP blocks.

5. Support for Cloud-Based Medical Systems

Support for cloud-based medical systems in CIDR involves efficiently managing IP addresses and routing for secure, scalable access to healthcare applications hosted in the cloud. By using classless addressing and CIDR prefixes, hospitals and clinics can create precise subnets for different departments, devices, or services, ensuring that sensitive patient data is isolated and securely routed. CIDR also enables route summarization and flexible network expansion, which is essential as medical systems grow or integrate multiple cloud services. This approach improves network performance, reliability, and security, making it easier for medical staff to access critical applications and patient records without interruptions or unauthorized access.

DOI: 10.46121/pspc.54.1.2

- Many online medical assessment platforms are hosted in the cloud.
- CIDR enables flexible IP allocation and smooth integration between cloud servers and healthcare networks.

Classless Inter-Domain Routing (CIDR) is a networking technique that allows flexible IP address allocation using variable-length subnet masks. In quick response systems for medical assessment—such as emergency triage platforms, online symptom checkers, or rapid diagnostic portals—CIDR plays an important supporting role.

Importance of CIDR in Medical Quick Response Systems

1. Fast Data Routing
- CIDR reduces routing table size, enabling faster packet forwarding.
- This is critical for quick response medical systems where delays can affect patient outcomes.

2. Efficient IP Address Utilization
- Medical quick response systems may experience sudden spikes in users.
- CIDR allows dynamic and efficient allocation of IP addresses without waste.

3. Network Scalability
- CIDR supports easy expansion when more assessment devices, mobile apps, or emergency units are added.
- New subnets can be created without redesigning the entire network.

4. Enhanced Security
- Sensitive medical assessment servers can be placed in isolated CIDR blocks.
- Access can be restricted to trusted IP ranges, reducing exposure to cyber threats.

5. Support for Cloud and Emergency Services
- Quick response systems often rely on cloud infrastructure.
- CIDR enables smooth integration between hospitals, ambulances, and cloud-based assessment platforms.

Example Use Case

A hospital emergency assessment system uses:

172.16.10.0/24
- /26 for emergency staff devices
- /27 for patient assessment kiosks
- /28 for backend analytics servers

This structured approach ensures rapid access, security, and efficient network performance.

Role of CIDR in IoT-to-Cloud Medical Data Collection

1. Efficient IP Address Allocation
- Large numbers of IoT medical devices need network access.
- CIDR allows flexible IP allocation (small or large subnets) based on device count, avoiding IP wastage.

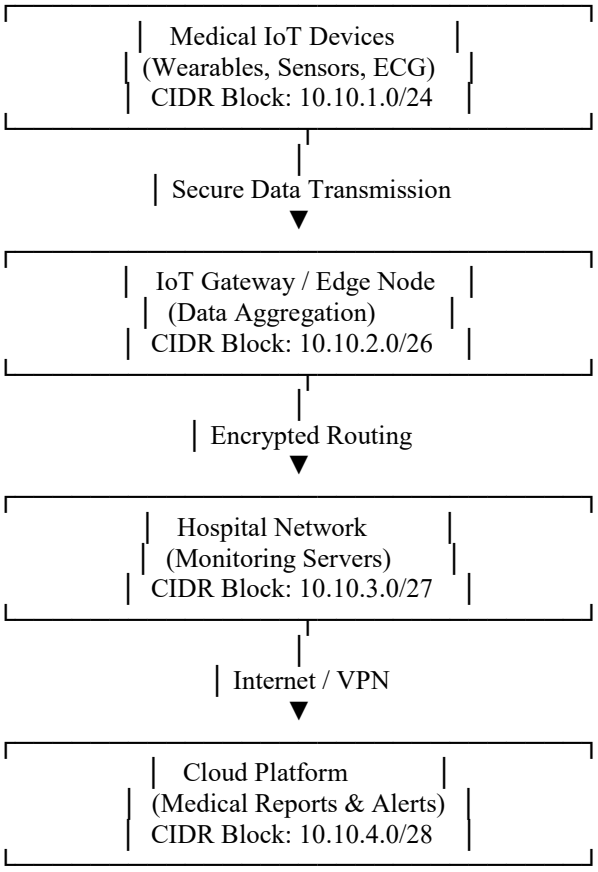
2. Scalable Device Integration
- New medical IoT devices can be added easily without changing the entire network.
- CIDR supports hierarchical subnetting for different hospital departments or device types.

3. Secure Data Transmission
- Medical data is sensitive and must be protected.
- CIDR enables network segmentation, isolating IoT devices from core hospital and cloud servers.

4. Optimized Routing to Cloud
- CIDR reduces routing table size, ensuring faster and more reliable data transfer from IoT devices to cloud platforms.
- This is essential for continuous monitoring and real-time report updates.

5. Cloud Compatibility
- Cloud providers use CIDR blocks for virtual networks.
- Medical IoT systems can integrate seamlessly with cloud virtual private networks (VPNs).

DOI: 10.46121/pspc.54.1.2



Preventing Pathway (Route) Hijacking in Networks
(Applicable to medical IoT, cloud systems, and surveillance networks)
Pathway hijacking (often called route hijacking) happens when an attacker advertises false routing information and diverts network traffic. In medical systems, this can expose or disrupt sensitive patient data.

Key Methods to Prevent Pathway Hijacking

1. Route Authentication
- Use RPKI (Resource Public Key Infrastructure) to verify legitimate IP route ownership.
- Prevents unauthorized networks from advertising fake routes.

2. Secure Routing Protocols
- Enable authentication in routing protocols (e.g., secure BGP configurations).
- Accept routes only from trusted peers.

3. CIDR-Based Route Filtering
- Allow only specific CIDR blocks that belong to known medical IoT devices and cloud servers.
- Reject unexpected or overly broad route announcements.

4. Network Segmentation
- Separate IoT devices, gateways, hospital servers, and cloud interfaces into different CIDR subnets.
- Limits damage if one segment is compromised.

5. Encryption of Data Paths
- Use VPNs or encrypted tunnels between IoT gateways and cloud servers.
- Even if traffic is redirected, data remains unreadable.

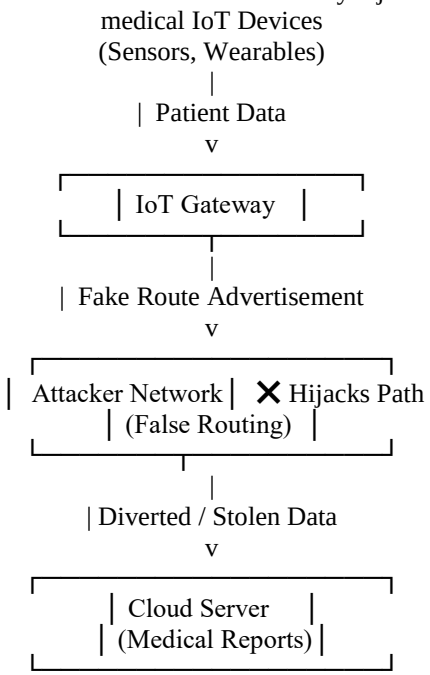
DOI: 10.46121/pspc.54.1.2

Power System Protection and Control
ISSN:1674-3415

6. Continuous Monitoring & Alerts
- Monitor routing changes and traffic paths in real time.
- Set alerts for abnormal route updates or sudden latency changes.

7. Firewall and Access Control Lists (ACLs)
- Configure firewalls to allow traffic only from trusted IP ranges.
- Block unauthorized routing announcements.

Example (Medical IoT Context)
- Only accept routes from:
- 10.20.0.0/16 (Hospital Network)
- 10.30.1.0/24 (IoT Gateways)
- Any external or unknown route advertisements are automatically rejected.



BGP (Border Gateway Protocol) Attacks in Medical Systems
BGP is the protocol used to exchange routing information between networks on the Internet. Medical networks rely on BGP indirectly for connecting hospital networks, IoT devices, and cloud servers. Attacks on BGP can disrupt connectivity or compromise sensitive patient data

1. Common BGP Attack Types

Attack Type	Description	Medical Impact
Route Hijacking	Attacker advertises IP prefixes they don't own. Traffic is diverted through attacker's network.	Patient data from IoT devices or hospital servers could be intercepted or delayed.
Route Leak	A network unintentionally announces routes learned from one provider to another.	Can cause data from medical monitoring systems to take longer paths, increasing latency for real-time assessments.
Prefix Squatting	Advertiser claims only a portion of an IP block they do not own.	Cloud servers or hospital devices may become unreachable.
BGP Interception	Traffic is diverted through attacker-controlled nodes but then forwarded to destination.	Allows stealthy eavesdropping of medical reports, lab results, or telemedicine communications.

2. Why Medical Networks Are Vulnerable
- Hospitals often connect to multiple ISPs for redundancy → increases attack surface.

DOI: 10.46121/pspc.54.1.2

- IoT devices continuously send patient data → sensitive targets.
- Cloud-based storage for reports relies on correct routing → BGP misconfiguration can disrupt patient care.

3. Prevention Strategies

1. **Route Authentication**
   - Use RPKI (Resource Public Key Infrastructure) to validate route announcements.

2. **CIDR-Based Filtering**
   - Only accept known IP blocks for IoT devices, hospital networks, and cloud servers.
   - Example: 10.20.0.0/16 for hospital internal network, 10.30.0.0/24 for IoT gateways.

3. **Network Segmentation**
   - Separate hospital networks, IoT devices, and cloud interfaces using CIDR subnets.

4. **Monitoring and Alerts**
   - Continuously watch BGP announcements. Trigger alerts for unexpected changes.

5. **Encryption of Medical Data**
   - Use VPNs or TLS tunnels so even if traffic is hijacked, data remains unreadable.

4. Example Scenario

- IoT heart monitors in a hospital (10.50.1.0/24) send patient data to cloud servers (10.50.2.0/24).
- An attacker advertises 10.50.2.0/24 via BGP → traffic is redirected.
- With RPKI + CIDR filtering + VPN, the hospital detects and blocks the false route, keeping data secure.

URGENT DATA

n medical diagnosis, “urgent data” refers to patient information that must be transmitted, processed, and acted upon immediately to ensure timely treatment. This includes critical measurements from IoT devices, lab results, imaging, or emergency alerts.

1. Types of Urgent Data

Type	Example	Importance
Real-time physiological data	Heart rate, oxygen levels, ECG from wearable IoT devices	Detect emergencies like arrhythmia, hypoxia
Laboratory results	Blood sugar, infection markers	Guide urgent treatment decisions
Imaging results	CT scans, X-rays	Critical for stroke, trauma, or emergency surgery
Alerts & notifications	Fall detection, emergency calls	Immediate response by healthcare staff

2. Characteristics of Urgent Data

- Low latency requirement – Must reach doctor or monitoring system in seconds/minutes.
- High reliability – No data loss allowed.
- Priority over routine data – Needs fast network routing and processing.
- Secure handling – Sensitive patient info must remain confidential even in emergencies.

3. Transmission in Medical IoT Systems

- IoT devices → Gateway → Cloud / Hospital Server
- Urgent data is often marked with high-priority tags for network Quality of Service (QoS).
- CIDR-based subnetting and route optimization can ensure urgent data avoids network congestion.
- Encryption (VPN/TLS) protects sensitive urgent medical info4. Example: Heart Monitor Alert

1. A wearable ECG detects a life-threatening arrhythmia.
2. Data is immediately transmitted via a secure IoT network using a high-priority path.
3. Cloud or hospital monitoring system alerts doctors/nurses.

DOI: 10.46121/pspc.54.1.2

4. Emergency response (medicine or intervention) is initiated

MILLION SQUARE ROUTING IN PATIENT MONITORING

Definition:

"Million Square Routing" refers to network designs and routing strategies that handle millions of connected devices (like IoT wearables, sensors, monitors) efficiently across a hospital, city, or region. The term emphasizes large-scale routing tables and subnet management for dense medical monitoring networks.

Million-square routing also refers to the ability of modern routing protocols and networks to efficiently handle extremely large numbers of routes, often in the range of millions, across the internet or large enterprise networks. This concept is especially important for ISPs and global networks where CIDR-based route aggregation and summarization help keep routing tables manageable despite the huge number of subnets. By combining multiple smaller networks into single summarized routes and using classless routing protocols, million-square routing improves scalability, performance, and reliability, ensuring that even very large and complex networks can forward traffic accurately without overwhelming routers or slowing down the network.

1. Purpose in Patient Monitoring

- Hospitals may have thousands of patients monitored continuously.
- Each patient may have multiple IoT devices: heart rate, oxygen, glucose, etc.
- Data must reach central servers or cloud for real-time monitoring.
- Efficient routing ensures low latency, no congestion, and secure delivery.

2. How CIDR Supports Million Square Routing

- CIDR subnetting allows flexible allocation of IP addresses to millions of IoT devices without wasting IP space.
- Example:
  10.0.0.0/8 → Entire hospital city network
  ├─ 10.1.0.0/16 → Hospital A IoT devices
  ├─ 10.2.0.0/16 → Hospital B IoT devices
  ├─ 10.3.0.0/16 → Remote patient home monitoring devices
- Each /16 can handle 65,536 devices, enabling scaling to millions.

3. Routing Techniques

1. **Hierarchical Routing**
   - Group devices by wards, floors, or hospitals.
   - Reduces routing table size and improves performance.

2. **Edge Routing**
   - IoT gateways aggregate patient data locally.
   - Only summarized or urgent data is sent to cloud servers, reducing network load.

3. **Priority Paths for Urgent Data**
   - Emergency alerts (e.g., heart attack) are routed on low-latency paths.
   - Non-urgent data (routine vitals) can use normal routes.

4. **Dynamic Routing Protocols**
   - BGP or OSPF with CIDR-based route aggregation.
   - Efficient handling of millions of devices.

DOI: 10.46121/pspc.54.1.2

Example Workflow
Patient Wearables (HR, BP, Oxygen)
▼ ▼Million square

IoT Gateway (Aggregates 1000s of devices)
CIDR: 10.1.1.0/22
▼
Hospital Server Network
CIDR: 10.1.0.0/16
▼
Cloud Analytics & Alert System
CIDR: 10.50.0.0/16

Million square routing allows millions of devices across multiple hospitals/cities to be managed efficiently using CIDR blocks and hierarchical routing.

5. Benefits

- Scalable: Supports millions of patient devices.
- Low latency: Urgent data reaches doctors immediately.
- Secure: Segmentation prevents unauthorized access.
- Efficient: Reduces routing table size with CIDR aggregation

CONCLUSION

CIDR enhances the reliability, speed, and security of quick response systems used in medical assessments. By optimizing IP routing and subnetting, CIDR helps ensure timely medical evaluations and effective .Million square routing is the fastest and secure routing specially for medical diagnosis and reporting. In conclusion, million-square routing demonstrates how modern networks can scale to handle millions of routes efficiently without sacrificing performance or reliability. By leveraging CIDR, route summarization, and classless routing protocols, networks can manage vast numbers of subnets while keeping routing tables compact and manageable. This approach ensures faster routing decisions, reduces congestion, and maintains stable connectivity, making it essential for large-scale internet service providers, enterprise networks, and cloud infrastructures. Ultimately, million-square routing highlights the importance of careful network design and advanced routing techniques in supporting today's highly connected and data-intensive world.

REFERENCES

1. Use of Short-Term CIDR-Based Protocols for Oestrus Synchronisation in Goats at Tropical and Subtropical LatitudesA Nakafeero, A Gonzalez-Bulnes, P Martinez-Ros - Animals, 2024 - mdpi.com
2. Efficiency of CIDR-Based Protocols Including GnRH Instead of eCG for Estrus Synchronization in Sheep
3. Efficiency of CIDR-Based Protocols Including GnRH Instead of eCG for Estrus Synchronization in Sheep by Paula Martinez-Ros ,Antonio Gonzalez-Bulne
4. Enhancing Efficiency In Computer Network Addressing, Urazimbetova A. Askarov U.
5. Effect of One-Day Delaying CIDR Administration in 5-Day Cosynch Protocol in Dairy Heifers by Sükrü Metin Pancarci Örsan Güngör Osman Harput Oguz Calisici
6. Evaluation of the Tuberculosis Surveillance System in Depok, West JavA, Fitri Aulia, Helda, Hidayat Nuh Ghazali Djadjuli

DOI: 10.46121/pspc.54.1.2