

**CONSUMER PROTECTION ASSOCIATION
HIMMATNAGAR
DIST. : SABARKANTHA
GUJARAT**



**Comments on
Consultation Paper on
Review of existing TRAI Regulations on Interconnection
matters**

Introduction :

1. Consumer-Centric Introduction

Interconnection is not merely a technical or commercial arrangement between telecom service providers; it is the **foundation of universal connectivity, consumer choice, affordability, service quality, and national digital inclusion**. From a consumer perspective, every voice call made, every SMS delivered, and every emergency communication attempted across networks depends entirely on the effectiveness, fairness, and reliability of interconnection frameworks.

India today supports over **1.2 billion telecom subscribers**, with mobile telephony as the primary mode of communication and an accelerating shift towards **data-driven services, OTT applications, A2P messaging, VoLTE/VoWiFi, and 5G**. In such an ecosystem, **interconnection failures**,

delays, discriminatory provisioning, or outdated cost and capacity models directly translate into call drops, congestion, service denial, inflated tariffs, and erosion of consumer trust. Therefore, the review of interconnection regulations is not only a regulatory or industry necessity—it is a **consumer protection imperative.**

The existing interconnection regulations were designed primarily in an era of **TDM/E1-based PSTN networks, hierarchical switching, and circuit-switched traffic models.** However, today's telecom landscape is fundamentally different—**IP-based networks, cloud-native cores, centralized switching, virtualization (NFV/SDN), 5G slicing, and IoT traffic** dominate the ecosystem. Continuing with legacy frameworks in such a transformed environment risks:

- Creating **artificial network bottlenecks,**
- Allowing **non-transparent inter-operator practices,**
- Delaying **service rollout,** and
- Ultimately harming **consumer experience, choice, and affordability.**

This consultation is therefore critically important from the consumer point of view to ensure that:

- **Interconnection is timely, non-discriminatory, transparent, and technology-neutral**
- **Costs saved through IP-based interconnection are passed on to consumers**
- **Quality of service (QoS) is protected across inter-operator boundaries**

- **Emergency and public safety communications remain fail-safe**
- **Competition is strengthened, not distorted by interconnection leverage**

The review must thus be guided by **four core consumer principles**:

1. **Universality** – Every consumer must be able to connect with any other consumer seamlessly.
2. **Affordability** – Interconnection costs must not inflate retail tariffs.
3. **Reliability & Resilience** – Networks must remain robust during disasters, congestion, and cyber threats.
4. **Transparency & Fair Competition** – No service provider should misuse interconnection for market dominance.

In this context, the present consultation is a timely opportunity to **modernize India’s interconnection regime in harmony with global best practices and emerging technologies**, while firmly anchoring it in **consumer welfare, digital inclusion, and long-term sector sustainability**.

2. Global Scenario on Interconnection Regulation (Consumer-Centric Perspective)

Across the world, telecom regulators have already transitioned their interconnection frameworks from **legacy circuit-switched models to IP-centric, competition-friendly, consumer-oriented regimes**. The global experience offers valuable lessons for India in terms of **regulatory design, technology migration, competition safeguards, and consumer protection outcomes**.

2.1 Evolution of Global Interconnection Frameworks

Internationally, the last two decades have witnessed:

- Migration from **TDM-based interconnection to SIP/IP-based interconnection**
- Shift from **geographical switching hierarchies to centralized IP cores**
- Replacement of **fixed port charges and per-circuit models with capacity- and QoS-based frameworks**
- Growing focus on **network neutrality, equivalence of inputs (Eol), and non-discriminatory access**

Global regulators now recognize that interconnection is no longer only about **voice termination**, but also about:

- **A2P messaging ecosystems**
- **Enterprise connectivity**
- **Emergency services**
- **Cross-platform interoperability**
- **Cybersecurity and lawful interception**

2.2 European Union (EU – BEREC & Ofcom Models)

- The **EU regulatory framework**, coordinated by **BEREC**, is built on:
 - **Equivalence of Inputs (Eol)**
 - **Cost-oriented wholesale access**
 - **Technology-neutral interconnection**
- Countries like the **UK (Ofcom)** require dominant operators to:

- Offer identical interconnection terms to competitors as to their own retail arms.
- Publish **Reference Interconnection Offers (RIOs)** with strict non-discrimination conditions.
- With full migration to **IP interconnection**, many EU nations have:
 - Eliminated **TDM-based POI structures**
 - Adopted **centralized IP handover**
 - Enabled **faster service innovation and lower retail prices for consumers**

Consumer Impact:

- * Reduced call termination costs
- * Faster rollout of new services
- * Improved voice quality (HD Voice/VoLTE)
- * Strong anti-discrimination enforcement

2.3 United States (FCC Framework)

- The US operates under a **technology-neutral interconnection regime** governed by:
 - The **Telecommunications Act**
 - **IP-to-IP Interconnection policies**
- The FCC encourages:
 - **Commercial negotiation backed by regulatory oversight**
 - **Interoperability between legacy PSTN and IP networks**
- With VoLTE and cloud interconnection now dominant, the US has:
 - Practically eliminated dependence on **traditional SS7-TDM POIs**

- Focused on **service interoperability, emergency access (NG-911), and reliability obligations**

Consumer Impact:

- High resiliency for emergency services
- Inter-carrier QoS accountability
- Innovation-driven competition without retail price escalation

2.4 Singapore (IMDA Model)

- Singapore mandates **all-IP interconnection** with:
 - Centralized IP gateways
 - Transparent wholesale pricing
- Interconnection is treated as **critical national digital infrastructure**.
- Strong regulatory focus on:
 - **Service continuity**
 - **Disaster resilience**
 - **Cybersecurity coordination across operators**

Consumer Impact:

- Near-zero call failure rates
- Seamless cross-operator VoLTE
- High trust in digital services

2.5 Australia (ACCC Framework)

- Australia has adopted a **structural separation and open-access interconnection model**.

- Interconnection at national IP exchange points is mandatory for dominant networks.
- Focus is placed on:
 - **Fair wholesale access**
 - **Transparent inter-operator dispute resolution**
 - **Strict QoS monitoring**

Consumer Impact:

- Stable inter-operator service quality
- Transparent wholesale pass-through pricing
- Consumer tariffs insulated from wholesale disputes

2.6 Japan & South Korea (Advanced IP & 5G Interconnection)

- Both countries operate **fully IP-native interconnection regimes**.
- Strong integration of:
 - VoLTE/VoNR
 - 5G core inter-operability
 - Data-centric interconnection charging frameworks
- Interconnection is linked with:
 - **Cyber-resilience**
 - **National security**
 - **Disaster recovery frameworks**

Consumer Impact:

- Ultra-low latency voice calls
- Superior indoor and cross-network coverage
- Extremely high service availability during disasters

2.7 Key Global Principles Emerging from International Practice

From a comparative consumer-centric analysis, the following **global best-practice principles** clearly emerge:

1. IP-First Interconnection:

All new interconnections are IP-based; TDM is being systematically retired.

2. Equivalence of Inputs (EoI):

Dominant operators must offer identical wholesale terms to competitors and their own retail arms.

3. Centralized Interconnection Models:

National or regional IP-level handover points replace SDCA/LDCA-level fragmentation.

4. Cost-Oriented & Transparent Charging:

Port and termination charges reflect actual network costs, not legacy infrastructure costs.

5. Strong Consumer QoS Enforcement:

Interconnection failures directly trigger regulatory penalties and consumer compensation.

6. Emergency & Disaster Resilience Embedded in Interconnection Rules:

Interconnection is treated as a public safety infrastructure.

Consumer-Centric Implication for India

India now stands at a **critical transition point similar to what the EU, US, Japan, and Singapore crossed over the last 10–15 years**. From a consumer standpoint:

- Continuing with **SDCA/LDCA and E1-centric models risks locking consumers into outdated quality and cost structures.**
- Delayed migration to **IP-centric interconnection may slow VoLTE, A2P innovation, 5G services, and IoT ecosystems.**
- Without strong **Eol-based non-discrimination safeguards**, interconnection can easily become a **tool for market foreclosure.**

Therefore, **global practice strongly supports India's regulatory review initiative** and reinforces the need for:

1. IP-native interconnection
2. Non-discriminatory access
3. Centralized POI models
4. Transparent cost frameworks
5. Strong consumer QoS protections

Comparative Global Interconnection Framework: Country vs Key Features vs Consumer Impact

Country / Region	Key Features of Interconnection Framework	Direct Consumer Impact
European Union (BEREC – UK, Germany, France, etc.)	<ul style="list-style-type: none"> • IP-based interconnection mandated • Equivalence of Inputs (Eol) enforced • Strict non-discrimination obligations on SMP operators • Centralized national/regional IP POIs • Cost-oriented wholesale pricing • Mandatory Reference Interconnect Offers (RIOs) 	<ul style="list-style-type: none"> • Lower retail tariffs due to cost-oriented wholesale access • Uniform service quality across networks • Faster rollout of VoLTE & broadband services • Strong protection against call blocking & discrimination
United Kingdom (Ofcom)	<ul style="list-style-type: none"> • Full migration to IP interconnection • Structural separation & Eol obligations on BT • National IP switching & centralized gateways • Mandatory wholesale QoS reporting 	<ul style="list-style-type: none"> • Significant reduction in call failures • Improved indoor voice quality (HD Voice) • Wholesale savings passed to retail consumers • Enhanced

Country / Region	Key Features of Interconnection Framework	Direct Consumer Impact
		accountability during network outages
United States (FCC)	<ul style="list-style-type: none"> • Technology-neutral IP-to-IP interconnection • Commercial negotiation backed by FCC oversight • NG-911 emergency interconnection framework • Cloud-based inter-carrier interconnect 	<ul style="list-style-type: none"> • Extremely high emergency call reliability • Seamless cross-carrier VoLTE • Rapid innovation in digital voice & enterprise services • Strong cyber-resilience for consumers
Singapore (IMDA)	<ul style="list-style-type: none"> • Mandatory all-IP interconnection • Centralized national IP interconnect gateway • Transparent wholesale interconnect pricing • Cybersecurity-integrated interconnection policy 	<ul style="list-style-type: none"> • Near-zero call drops • Uniform VoLTE across all operators • High reliability for digital public services • Strong consumer trust in telecom networks
Australia (ACCC)	<ul style="list-style-type: none"> • Structural separation of wholesale & retail • Mandatory open-access interconnection • National broadband IP interconnection • Strict QoS compliance audits 	<ul style="list-style-type: none"> • Uniform rural & urban service quality • Lower inter-operator disputes reflected in stable tariffs • Strong consumer grievance resolution
Japan	<ul style="list-style-type: none"> • Full IP-native interconnection • Ultra-high capacity centralized interconnect • Strong disaster-resilient interconnect architecture • 5G-native inter-operator integration 	<ul style="list-style-type: none"> • Ultra-low latency voice & data • Network availability even during disasters • Superior consumer QoE for mobility & broadband
South Korea	<ul style="list-style-type: none"> • Fully virtualized interconnection (NFV & SDN) • 5G & VoNR-native interconnection • Centralized IP traffic routing • Disaster-grade telecom resilience 	<ul style="list-style-type: none"> • Seamless VoNR & HD voice • Zero black-spots between operators • Extremely high service reliability
New Zealand	<ul style="list-style-type: none"> • Mandatory Equivalence of Inputs (EoI) • Centralized IP-based interconnect • Open wholesale access to incumbent infrastructure 	<ul style="list-style-type: none"> • Competitive retail pricing • Faster broadband & VoIP service rollout • Non-discriminatory inter-operator QoS
Canada	<ul style="list-style-type: none"> • IP-centric interconnection • SMP-based wholesale price regulation • Mandatory call completion standards 	<ul style="list-style-type: none"> • Consistent rural connectivity • High emergency call

Country / Region	Key Features of Interconnection Framework	Direct Consumer Impact
	• Emergency service prioritization over interconnect	reliability • Transparent wholesale-to-retail cost flow
European Nordic Countries (Sweden, Finland, Norway)	• 100% IP interconnection • National centralized switching • No TDM-based POIs • Strong cyber & disaster resilience	• Highest global telecom QoS • Minimal outage impact on consumers • Stable broadband & voice tariffs

TRAI-Specific Alignment Matrix: Global Best Practice → Indian Regulation Gaps → Consumer Impact & Regulatory Direction

Global Best Practice	Current Position under Indian Interconnection Regulations	Consumer-Centric Gap Identified	Suggested Direction for TRAI (Consumer-Oriented)
1. Mandatory All-IP Interconnection (EU, Japan, Singapore)	Indian interconnection still legally anchored to TDM/E1, SDCA/LDCA-based POIs , though IP networks coexist (TIR 2018 + RIO 2002).	Dual TDM-IP regime causes inefficiency, congestion risk, higher costs , and delays in high-quality VoLTE/VoWiFi services.	Introduce time-bound nationwide migration to mandatory IP-to-IP interconnection with phased sunset of TDM POIs, ensuring cost savings are passed to consumers.
2. Centralized National/LSA-Level IP POIs	Fixed wireline largely at SDCA/LDCA levels , wireless already at LSA level .	Artificial geographic fragmentation leads to route inefficiencies, higher interconnect cost → higher retail tariffs .	Mandate LSA-level centralized IP POIs for all PSTN/PLMN interconnection , with limited exceptions only by mutual agreement.
3. Equivalence of Inputs (EoI) for Dominant Operators (EU, NZ, UK)	Non-discrimination principle exists, but no explicit EoI obligation in Indian interconnection framework.	Risk of preferential treatment to own retail arms , delayed provisioning to competitors → reduced competition → higher consumer prices.	Explicitly embed Equivalence of Inputs (EoI) in TIR and RIO, with real-time compliance audits and penalties.

Global Best Practice	Current Position under Indian Interconnection Regulations	Consumer-Centric Gap Identified	Suggested Direction for TRAI (Consumer-Oriented)
4. Cost-Oriented & Transparent Interconnection Charges (EU, Australia)	Legacy port-based charging models , linked historically to E1/TDM cost structures.	Charges may not reflect actual IP network costs , leading to distorted wholesale pricing and hidden consumer burden.	Replace legacy port-charge logic with IP-capacity & QoS-based cost models , with mandatory wholesale-to-retail pass-through transparency.
5. Fast, Time-Bound Interconnection Provisioning (UK, Singapore)	30-day agreement window exists in TIR 2018, but enforcement is weak and dispute-prone .	Delays in interconnection directly cause call failures, launch delays, and consumer service denials .	Introduce automatic deemed approval, hard provisioning SLAs, and consumer-linked financial disincentives for delay.
6. Centralized Public Interconnect Disclosure & Dashboards (EU, FCC)	Register of Interconnect Agreements exists (1999), but not real-time, not consumer visible .	Consumers lack visibility into inter-operator bottlenecks that cause QoS failures .	Create a TRAI Interconnection Transparency Portal : POI congestion, provisioning delays, and dispute status made public.
7. Disaster-Resilient & Emergency-Priority Interconnection (US NG-911, Japan)	Emergency call priority exists, but interconnection resiliency is not explicitly embedded as a disaster-grade framework .	Natural disasters and outages still result in cross-operator call failures , harming public safety.	Mandate multi-path resilient IP interconnection , geo-redundant POIs, and emergency-first routing obligations.
8. Interconnection & Cybersecurity Integration (Singapore, EU)	Cybersecurity addressed separately from interconnection regulations.	Growing IP interconnection attack surface exposes consumers to large-scale outages and fraud.	Integrate cyber-resilience standards, encrypted SIP interconnect, and inter-operator security audits within interconnection rules.
9. Technology-Neutral, Data-Centric	Current framework is still voice-centric and SMS-centric .	India's traffic is now data-dominated , yet interconnection	Shift to unified IP interconnection rules covering voice, A2P messaging,

Global Best Practice	Current Position under Indian Interconnection Regulations	Consumer-Centric Gap Identified	Suggested Direction for TRAI (Consumer-Oriented)
Interconnection Frameworks		law remains voice-legacy-oriented .	enterprise data, IoT, and future NTN/satellite interconnect.
10. Strong Wholesale QoS Enforcement Linked to Retail Consumer Outcomes	QoS largely monitored at retail network level, not at interconnection layer .	Inter-operator congestion directly degrades call quality without clear consumer remedies .	Introduce interconnection-level QoS benchmarks with consumer compensation triggers for persistent violations.
11. Structural Separation or Functional Firewalls for Dominant Operators (UK, Australia)	No formal structural separation in Indian interconnection context.	Risk of leveraging interconnection dominance to suppress competition , impacting tariffs and innovation.	Impose functional separation safeguards in interconnection provisioning, POI allocation, and traffic routing .
12. Simplified & Consolidated Interconnection Codes (EU)	India operates under multiple legacy regulations (1999–2018) with overlapping provisions.	Regulatory complexity leads to delay, litigation, and compliance ambiguity , harming consumer interests.	Consolidate into a Unified Indian Interconnection Code , fully IP-native and consumer-oriented.
13. Real-Time Dispute Resolution Mechanisms (UK, Australia)	Disputes often escalate to TDSAT or Courts , causing long delays.	Consumers suffer prolonged QoS issues while operators litigate.	Create a fast-track technical arbitration cell within TRAI exclusively for interconnection disputes.
14. A2P Messaging & Enterprise Traffic Interconnection Regulation (Global Trend)	SMS termination rules exist (2013), but A2P ecosystem is weakly integrated into IP interconnection logic .	A2P misuse, spam, and delivery failures directly affect consumers and enterprises .	Establish a dedicated IP-A2P interconnection framework with traceability, QoS assurance, and fraud prevention.
15. Satellite & NTN Interconnection	Current interconnection regulations do not	Upcoming satellite-mobile services could face	Introduce future-ready interoperable interconnection

Global Best Practice	Current Position under Indian Interconnection Regulations	Consumer-Centric Gap Identified	Suggested Direction for TRAI (Consumer-Oriented)
Readiness (Global 5G-NTN Future)	fully address NTN/MSS/FSS interworking.	interconnect bottlenecks harming rural consumers.	standards for satellite-terrestrial integration.

Core Regulatory Insight from the Alignment Matrix (Consumer View)

The alignment analysis clearly indicates that **India's interconnection framework remains structurally rooted in legacy circuit-switched assumptions**, while global practice has already transitioned to **fully IP-centric, consumer-centric, transparency-driven interconnection regimes**.

Unless India undertakes **timely, decisive, and consumer-oriented modernization**, the following risks will persist:

- Structural inefficiencies will **inflate consumer tariffs**.
- Inter-operator disputes will continue to **affect call quality and service availability**.
- IP-native services (VoLTE, 5G, A2P, IoT, Satcom) will suffer from **legacy regulatory drag**.
- Emergency communication reliability will remain **sub-optimal under disaster conditions**.

Issues for Consultation

A. Regulations-wise Specific Questions

A.1. The Telecommunication Interconnection Regulations, 2018

Q1. For PSTN to PSTN, PLMN to PSTN and PSTN to PLMN, should the interconnection level be specified at LSA level? If yes, should the existing POIs at the LDCA/SDCA level also be migrated to the LSA level? Kindly justify your response.

Comments :

1. Should the interconnection level be specified at the LSA level? —

Conditional Yes, with safeguards

Specifying interconnection at the **Licensed Service Area (LSA)** level can support harmonisation and reduce unnecessary duplication of interconnection points. This may result in:

Potential Consumer Benefits

1. Better Call Quality & Fewer Call Drops

Consolidated POIs at the LSA level can improve traffic handling efficiency, resulting in more stable interconnection and fewer failed calls during peak hours.

2. Lower Cost of Network Interconnection (Eventually Lower Tariffs)

When operators reduce the number of physical POIs, operational costs fall. In a well-regulated tariff environment, these savings should flow to consumers as:

- affordable call tariffs
- better value packs
- reduced burden of termination charges

3. Greater Transparency and Simplification

Presently, POIs at SDCA/LDCA levels create technical complexity. LSA-level interconnection improves monitoring and compliance,

allowing TRAI to better detect congestion and misuse, ultimately helping consumers receive fair service.

2. Should the existing POIs at LDCA/SDCA level be migrated to the LSA level? — *A Cautious, Phased Approach is Required*

A blanket, immediate migration of all POIs to LSA level **may harm consumers**, especially in rural and semi-urban regions. The following consumer risks must be carefully considered:

Potential Risks to Consumers

1. Risk of Higher Retail Tariffs

Operators may argue that dismantling SDCA/LDCA POIs requires new investments at the LSA-level. Without safeguards, some operators may pass these costs to consumers, increasing call rates.

2. Risk of Reduced Local Access & Rural Connectivity

LDCA/SDCA level POIs currently support:

- local call routing
- reduced latency
- localised redundancy

Migrating everything to LSA-level may centralise the interconnection too much and degrade service quality in remote areas.

3. Risk of Increased Network Congestion if Local Points Removed

Removing local POIs without proportional investment in LSA-level capacity can cause longer routing paths, possibly leading to **call failures, echo, and delay**—issues directly affecting end consumers.

4. Unequal Impact on Small Operators

Smaller regional operators rely heavily on local POIs. Forcing them to migrate might reduce competition, which ultimately increases consumer prices.

3. Consumer-Oriented Justification: A Balanced Middle Path

To protect consumer interest, **a hybrid approach** is recommended:

✓ **Keep LSA-level interconnection as the *primary* standard,**

but ✓ **retain existing SDCA/LDCA POIs wherever they serve genuine consumer needs**, especially in:

- rural / geographically large LSAs
- areas with lower fiber penetration
- places where PSTN still carries significant traffic

✓ **Migration to LSA level should be phased, not mandatory, and must follow:**

- transparent cost-benefit assessment
- no increase in retail tariffs
- measurable improvement in call quality

TRAI may also direct that **any operator savings from POI consolidation must not lead to consumer tariff hikes**, ensuring accountability.

4. Final Recommendation (Consumer-First Summary)

Yes, interconnection at LSA level *may* be specified as a standard **only if**:

- it leads to measurable improvement in call quality and reliability,
- does not increase consumer tariffs,
- does not weaken rural connectivity, and
- is implemented gradually with continuous monitoring.

No blanket migration of existing LDCA/SDCA POIs should be mandated. Instead, apply a **case-by-case, consumer-centric phase-out**, ensuring that:

- local resilience is preserved,
- small operators remain competitive, and
- rural consumers are not disadvantaged.

Conclusion

Consumer interest must remain the core criterion. Interconnection should be designed to deliver **better quality, greater affordability, and equitable access** to all—urban and rural, PSTN and PLMN users alike. A cautious, phased shift toward LSA-level interconnection—supported by strong safeguards—achieves this balance more effectively than a uniform mandatory migration.

Q2. For PSTN to PSTN, PLMN to PSTN, PSTN to PLMN and PLMN to PLMN, should interconnection be allowed at a level other than the LSA level, based on mutual agreement? Kindly justify your response.

Comments :

Our response focuses on **consumer interest**, including affordability, service reliability, transparency, and universal access.

1. Should interconnection at levels other than LSA be permitted by mutual agreement?

Yes — but only with strict consumer-protection safeguards.

Allowing flexibility beyond the LSA level can promote innovation and reduce congestion, but unrestricted bilateral agreements may create risks for consumer rights, price fairness, and network resilience.

Therefore, any deviation from LSA-level interconnection should be:

- **Optional**, not mandatory
- **Transparent**, not private or opaque
- **Regulated**, not solely based on operator negotiations
- **Consumer-oriented**, not cost-shifting

2. Potential Consumer Benefits of Allowing Interconnection Below or Beyond LSA Level

a) Improved Call Quality & Lower Congestion

Operators may set up:

- SDCA-level or LDCA-level interconnection where traffic is high
- Metro-hub interconnection where routing is more efficient

This can reduce:

- call drops
- call set-up delays
- voice distortion and echo

Outcome: More reliable voice service for consumers.

b) Faster Rollout of Services

New operators or expanding networks may prefer interconnection at:

- district level
- city-specific POIs
- local trunk exchanges

Such flexibility can accelerate:

- service activation
- rural expansion
- inter-network connectivity

Outcome: Consumers receive services earlier and with fewer delays.

c) Lower Operational Costs & Potential for Affordable Tariffs

If two operators agree to interconnect at a technically efficient alternative point:

- infrastructure duplication reduces
- backhaul cost decreases
- operational savings rise

If TRAI mandates pass-through of efficiencies, **consumers benefit through affordable tariffs and better prepaid value.**

3. Potential Consumer Risks of Allowing Such Flexibility

a) Uneven Access and Regional Discrimination

If interconnection depends only on bilateral agreements:

- smaller operators may be denied favourable POIs
- rural or low-revenue areas may be ignored
- high-cost POIs may be forced on small providers

This harms competition and ultimately raises consumer prices.

b) Reduced Regulatory Oversight

Allowing unrestricted flexibility may:

- create opaque bilateral network arrangements
- make it harder for TRAI to monitor congestion
- conceal anti-competitive POI practices

Consumers may suffer from poor call quality without a clear accountability trail.

c) Risk of Higher Consumer Tariffs

Operators may:

- charge each other higher carriage for non-LSA interconnection
- pass these costs to consumers
- introduce hidden or complex tariff components

Outcome: Consumers pay more without benefiting.

d) Fragmentation of Interconnection Architecture

If too many arbitrary POIs emerge:

- troubleshooting becomes harder
- fault rectification is delayed

- emergency routing may get affected

This adversely impacts consumer safety and service reliability.

4. Consumer-First Justification: A Balanced Way Forward

✓ Allow interconnection at non-LSA levels, BUT only if the following conditions are met:

1. Complete transparency to TRAI

All non-LSA interconnection agreements must be filed with TRAI for oversight.

2. No additional cost passed on to consumers

Any deviation must not result in:

- tariff increase
- higher termination charges
- discriminatory pricing

3. Justification of technical or consumer advantage

Operators must demonstrate that such interconnection will:

- improve call quality
- reduce congestion
- expand coverage
- benefit consumers directly

4. Non-discrimination clause

All operators should have equal and fair access to alternative interconnection levels.

5. Safeguards for rural consumers

No operator should discontinue local SDCA/LDCA interconnection where it is essential for rural reliability.

5. Final Recommendation (Consumer-centric summary)

Interconnection at levels other than LSA may be permitted only under a regulated, transparent, and consumer-protective framework.

This flexibility:

- **can improve call quality, accelerate rollout, and reduce costs,**
- **but can also lead to uneven access, reduced oversight, and possible consumer price increases** if left unchecked.

Therefore:

✓ Yes — allow alternative interconnection levels

but only with strong TRAI safeguards ensuring:

- transparency
- no tariff increase
- non-discriminatory access
- protection of rural connectivity
- strict QoS monitoring

This achieves both network efficiency and **consumer protection**, ensuring that India's telecommunication ecosystem remains competitive, affordable, and aligned with public interest.

Q3. Based on your response to Question 1 and 2 above, what changes, if any, are required in the level of interconnection / point of traffic handover as provided in the following:

a) Telecommunication Interconnection Regulations (TIR), 2018, and

b) Guidelines annexed to the Telecommunication Interconnection (Reference Interconnection Offer) Regulations, 2002? Kindly justify your response.

Comments :

1. Overall consumer-centric position

From a consumer standpoint, **only limited, calibrated changes** are required in TIR 2018 and the RIO 2002 Guidelines, mainly to:

- Clarify **LSA-level** as the *default* reference level for interconnection and hand-over,
- Explicitly **allow flexibility** to use other levels (LDCA/SDCA or higher aggregation) where it **improves consumer welfare**, and
- Build strong **safeguards on transparency, non-discrimination, QoS, and tariff impact**.

The objective should *not* be to completely redesign the interconnection framework, but to **refine and update it** so that:

- Call quality improves,
- Affordability is preserved or enhanced,
- Rural and low-income users are not left behind, and
- Consumers can benefit from technological and network efficiencies.

2. Suggested changes in TIR 2018 (level of interconnection / POI)

2.1. Explicitly define LSA-level as the standard / default level

TIR 2018 may be amended to:

- Explicitly state that **LSA-level interconnection** is the **standard reference level** for PSTN–PSTN, PSTN–PLMN and PLMN–PLMN interconnection.
- Clarify that this is done primarily to:
 - ensure **predictability**,
 - simplify monitoring and QoS enforcement, and
 - prevent arbitrary or discriminatory interconnection practices.

Consumer benefit:

A clear default level helps TRAI monitor congestion and QoS more effectively and ensures every consumer, regardless of operator, enjoys a minimum standard of connectivity.

2.2. Introduce a flexibility clause for interconnection at other levels (below or above LSA)

In line with Q1 & Q2 responses, TIR 2018 may:

- **Permit interconnection at levels other than LSA** (e.g., LDCA/SDCA, or higher aggregation points),
- But **only under regulated conditions**, such as:
 - Mutual agreement **filed with TRAI**,
 - Demonstrated **technical or consumer benefit** (better quality, faster rollout, lower cost),
 - **No increase in retail tariffs** attributable to such arrangements, and
 - **Non-discriminatory access** for similarly placed operators.

Consumer benefit:

Flexibility allows operators to design efficient, innovative interconnection models that can reduce congestion and cost, which—if properly regulated—translates into better call quality and stable/affordable tariffs.

Consumer risk if not regulated:

Without such conditions, bilateral deals could lead to hidden costs, exclusion of smaller operators, and eventual tariff increases. Hence the conditions are critical.

2.3. Protection for rural and low-traffic areas

TIR 2018 may include a **specific safeguard** that:

- Existing **SDCA/LDCA-level POIs** serving rural / remote areas **must not be withdrawn** unless equivalent or better QoS can be ensured via LSA-level or alternative arrangements,
- TRAI may insist on a **consumer impact assessment** (QoS + tariff) before allowing such migration.

Consumer benefit:

Prevents rural users from experiencing degraded service (longer routes, higher latency, more drops) just because POIs are centralised for cost reasons.

2.4. Stronger transparency & reporting obligations

TIR 2018 could require that:

- All interconnection arrangements **not strictly at LSA-level** be **reported to TRAI**, including:

- physical handover points,
- capacity provisioning,
- congestion metrics, and
- any special charging arrangements.
- TRAI may periodically publish **aggregated, anonymised information** on interconnection QoS, so consumers know whether poor quality is due to congestion, routing, or other controllable factors.

Consumer benefit:

Better transparency ensures that quality issues are identified quickly and corrective action is taken in time, protecting the consumer's right to reliable service.

3. Suggested changes in RIO 2002 Guidelines (Reference Interconnection Offers)

The RIO Guidelines should be updated to align with the above principles and modern network realities.

3.1. Update RIO templates to reflect LSA-level as default, with optional additional levels

The RIO guidelines may be modified to require that:

- Every operator's RIO clearly specifies:
 - **Default (LSA-level) interconnection points**, and
 - **Optional additional levels** of interconnection (e.g., SDCA/LDCA, higher aggregation points), along with conditions.
- The RIO should provide **clear, non-discriminatory technical and commercial terms** for such additional interconnection levels.

Consumer benefit:

By standardising the way interconnection options are presented and offered, competition is protected, network efficiency improves, and consumers indirectly get better quality and pricing.

3.2. Mandatory consumer impact consideration in RIO modifications

When operators modify their RIOs to change POIs or levels of interconnection, guidelines may require that:

- They submit a **short consumer-impact note** to TRAI, covering:
 - expected impact on QoS,
 - any risk to rural / low-traffic areas,
 - assurance that **retail tariffs will not be increased** because of the change.
- TRAI may intervene if changes are likely to:
 - reduce access in certain regions,
 - weaken competition, or
 - indirectly increase consumer tariffs.

Consumer benefit:

Ensures that interconnection is not treated as a purely commercial/technical matter, but as one having direct impact on consumer rights and therefore subject to scrutiny.

3.3. Strengthen non-discrimination and fairness clauses

RIO guidelines may be refined to clarify that:

- If an operator offers a certain interconnection level (e.g., SDCA-level or special hub-level) to one operator, it should:
 - offer **similar terms** to other similarly placed operators,
 - avoid hidden or preferential arrangements that indirectly harm competition and consumer welfare.

Consumer benefit:

Healthy competition is the best long-term protection for consumers against high tariffs and poor service. Non-discriminatory RIO terms keep the playing field level.

4. Risks of making changes – and how to mitigate them

4.1. Transition costs and network reconfiguration

Risk:

Any change in TIR or RIO rules may require network planning, migration of POIs, and renegotiation of agreements, creating short-term costs.

Mitigation (consumer-centric):

- Provide a **reasonable transition period**,
- Avoid mandatory migration of all existing POIs,
- Allow **grandfathering** of some local POIs where they serve critical consumer needs.

4.2. Uneven implementation

Risk:

Larger operators may adapt quickly, while smaller operators may struggle, potentially weakening competition.

Mitigation:

- TRAI may issue **implementation guidelines** and possibly **handholding / advisory support** for smaller operators,
- Ensure that flexibility clauses are not misused to deny fair interconnection to small / regional providers.

5. Conclusion: Balanced justification in consumer interest

In light of our responses to Questions 1 and 2:

- **Yes, certain targeted changes** are required in **TIR 2018** and **RIO 2002 Guidelines**,
- But these changes should **refine and clarify** the framework rather than overhaul it.

Key principles to embed:

1. **LSA-level as the default**, reference level of interconnection and traffic handover;
2. **Regulated flexibility** to use other levels (lower or higher) where it demonstrably benefits consumers;
3. **No adverse impact on retail tariffs** and **no dilution of rural access**;
4. **High transparency, strong non-discrimination, and effective TRAI oversight.**

Such an approach:

- Enhances **call quality and reliability**,
- Protects or improves **affordability**,

- Preserves and strengthens **accessibility for rural and vulnerable consumers**, and
- Ensures that the **interconnection framework evolves with technology** while keeping consumer protection at its core.

This, in our view, best upholds the mandate that telecom regulation must ultimately serve the interests of Indian consumers.

Q4. Is there a need to mandate multi-path resiliency and redundancy in the Point of Interconnection (POI) framework to mitigate link failure at the primary POI in the case of:

- i. **PSTN-PSTN interconnection,**
- ii. **iii. PLMN-PLMN interconnection, and PLMN-PSTN interconnection? If yes, kindly provide an appropriate architectural framework with diagram. Kindly justify your response.**

Comments :

Response on Mandating Multi-Path Resiliency and Redundancy in the POI Framework for PSTN–PSTN, PLMN–PLMN, and PLMN–PSTN Interconnections

1. Consumer-Centric Rationale for Redundancy

Mandating multi-path resiliency and redundancy in interconnection is not merely a network-engineering concern; it is a **consumer-rights obligation**. As India transitions toward **Next-Generation Networks (NGN)** with rapidly expanding voice, data, and digital-service dependencies, consumers expect:

- **High reliability** (minimal call drops and service outages)
- **Affordability** (efficient interconnection reduces cost inflation)
- **Safety** (always-available connectivity for emergency services)
- **Digital trust** (confidence that networks are robust, continuous, and secure)

Redundancy—across access networks, transit networks, and Points of Interconnection (Pols)—is the foundational enabler of these goals.

Why Redundancy is Essential

1. Reliability:

A single-path interconnection creates a “single point of failure.” In the era of VoLTE/VoNR, even minor failures can disable large traffic zones.

2. Affordability:

Efficient congestion management through failover and multi-path routing reduces the need for emergency capacity procurement, which protects consumers from hidden inflationary pass-throughs.

3. Public Safety & Emergency Connectivity:

Redundant paths ensure **lifeline continuity** for 112/108 emergency calls during fibre cuts, equipment faults, or natural disasters.

4. Digital Trust:

Consumers associate stable connectivity with trust in digital payments, telemedicine, remote education, and financial transactions.

Thus, redundancy is both a **technical necessity** and a **consumer-protection mechanism**.

2. Scope: PSTN–PSTN, PLMN–PLMN, PLMN–PSTN

The requirement for multi-path redundancy should apply across:

i) PSTN–PSTN Interconnection

- Still relevant for rural and enterprise fixed lines
- Ensures continuity during copper-to-fibre transition

ii) PLMN–PLMN (Mobile-to-Mobile)

- India's dominant traffic segment (90%+)
- High stakes for reliability due to VoLTE/VoWiFi dependency

iii) PLMN–PSTN

- Critical for enterprise trunks, SMEs, call centres, and banking applications
- Redundancy ensures business continuity and prevents economic losses

3. Proposed Multi-Path Resilient POI Architecture

A modern, industry-ready architecture can be built on:

- **SDN (Software-Defined Networking)** for centralised control
- **NFV (Network Function Virtualisation)** for virtual POIs (vPOIs)
- **Dynamic Failover & Load Balancing**
- **Geo-Redundant POIs** (minimum two per LSA or cluster)
- **IP-based interconnect with MPLS/Segment Routing** for predictable performance

4. Functional Features

1. Multi-path routing:

At least two independent physical paths between networks.

2. Virtual POIs (vPOIs):

Dynamically scale during peak seasons (festivals, disasters).

3. Automatic failover:

<50 ms switchover using link-state change detection.

4. Geo-redundancy:

At least two POIs separated by 20–50 km to reduce correlated failures.

5. QoS-based traffic management:

Priority handling for emergency services, financial transactions, and enterprise-critical calls.

6. DDoS and congestion isolation:

Using network slicing and traffic-shaping.

5. Consumer Benefits

1. Near-Zero Call Drops

- Redundant paths eliminate interconnection failures.
- Especially important for VoLTE/VoNR where fallback to 2G/3G is declining.

2. Faster Recovery

- Virtualized POIs can be spun up within minutes.
- Disaster-resilient design protects consumers during cyclones, floods, and fibre-cuts.

3. Fair and Stable Pricing

- Lower unplanned CapEx and OpEx due to automation.
- Prevents tariff shocks passed to consumers due to inefficient interconnection cost overruns.

4. Improved Emergency Response

- Ensures 100% reachability for emergency numbers.
- Supports nation-wide alerts and public safety communication.

5. Strengthened Digital Trust

- Supports digital payments, telemedicine, online education, OTT calling, and cloud-based enterprises.

6. Risks and Challenges

1. Cost Implications

- Additional fibre routes
- Hardware for redundant POIs
- SDN controllers and NFV infrastructure

2. Operational Complexity

- Multi-operator coordination
- Fault diagnostics in multi-path scenarios
- Security and interoperability across diverse networks

3. Legacy PSTN Constraints

- Older TDM-based systems may need gateways or gradual migration

7. Safeguards and Mitigation Strategies

1. Phased Implementation:

- **Phase-1:** Mandate redundancy for LSA with high traffic and metro circles
- **Phase-2:** Rollout to all LSAs
- **Phase-3:** Introduce mandatory virtual POIs (vPOIs)

2. Cost-Sharing Framework:

- Operators may share passive and active infrastructure
- TRAI may specify cost-allocation norms to avoid consumer burden

3. Performance Indicators:

- Introduce “Interconnection Resiliency KPIs” in QoS regulations
- Monitor failover performance, POI congestion, and downtime

4. Interoperability Standards:

- Mandate open standards (SIP-I, VoLTE IMS interconnect, SR-MPLS)

5. Security Requirements:

- DDoS protection, secure routing, and mutual authentication of vPOIs

8. Alignment with Global Best Practices

International regulators have formalized multi-path resiliency as a core telecom obligation:

- **FCC (USA):** Disaster-resilient routing & network redundancy
- **Ofcom (UK):** Multi-operator exchange redundancy and resilient backhaul

- **EU BEREC:** Redundant interconnection for emergency services and VoIP

India can adopt a “**progressive compliance model**” aligned with these frameworks to support its growing digital economy.

9. Conclusion (Balanced Justification)

Mandating multi-path redundancy in interconnection—across PSTN-PSTN, PLMN-PLMN, and PLMN-PSTN—is not an operator-centric requirement but a **consumer-centric mandate** essential for:

- network reliability
- emergency safety
- affordability & fairness
- digital trust and inclusion
- resilience in natural disasters
- smooth migration to IP-based networks

While cost and operational complexity are real concerns, they are **manageable** through SDN/NFV-enabled automation, infrastructure sharing, and **phased implementation**. A resilient interconnect architecture is a foundational investment for India’s digital future and directly aligned with global standards and the rights of Indian consumers.

Therefore, adopting a regulated multi-path resilient interconnection framework is necessary, justified, and in the long-term interest of consumers and the telecom ecosystem.

Q5. Is there a need to incorporate security provisions in the interconnection framework to ensure network security? If yes, kindly provide details along with an appropriate architectural diagram. Kindly justify your response.

Comments :

Response on Incorporating Security Provisions into the Interconnection Framework for PSTN–PSTN, PLMN–PLMN, and PLMN–PSTN Networks

1. Consumer-Centric Rationale for Mandatory Interconnection Security

As India's telecom ecosystem transitions toward all-IP, VoLTE/VoNR-centric networks, the interconnection layer becomes the **most critical shared space** between operators. If left unprotected, this shared layer becomes a high-value target for:

- call hijacking
- spoofing and SPIT/robocalling
- signaling manipulation
- interconnection-focused DDoS attacks
- data leakage
- fraudulent termination
- emergency service disruption

Consumers ultimately bear the consequences: poor reliability, financial loss, privacy breaches, tariff distortions, and reduced trust in digital platforms.

Therefore, a **secure, zero-trust, standards-aligned interconnection framework** is essential for protecting consumer rights, ensuring service continuity, and sustaining India's digital growth.

2. Why Security Must Be Built Into Interconnection

i) Reliability

Security breaches at interconnection points can disable entire LSAs, cause mass call drops, and disrupt emergency services.

ii) Affordability

Fraud—CLI spoofing, interconnect bypass, grey routes—causes revenue leakage that eventually increases consumer tariffs. Stronger security reduces the burden of fraud-related inefficiencies.

iii) Digital Trust & Safety

Consumers expect their voice traffic to be private, authenticated, and protected from spoofing. A secure interconnect ensures confidence in digital payments, telemedicine, banking OTPs, and emergency access.

iv) National Security

Interconnects are high-value national assets. Strengthening them aligns with CERT-In and DoT cyber-resilience goals for critical infrastructure.

3. Security Provisions to be Incorporated in the Interconnection Framework

The following provisions should be mandated across PSTN–PSTN, PLMN–PLMN, and PLMN–PSTN interconnections:

1. Mutual Authentication

- Certificate-based authentication (PKI) between networks
- Prevention of unauthorized signaling endpoints
- Automatic rejection of untrusted traffic

2. End-to-End Encryption

- SIP/SIP-I over TLS for signaling
- SRTP for media paths
- IPsec/MPLS VPNs for inter-operator backbone communication

3. Zero-Trust Principles

- No implicit trust between operators
- Verification of identity, integrity, and authorization for every session
- Least-privilege access to interconnection resources

4. Secure Signaling Architecture

- SIP-I, Diameter, and MAP firewalls
- Validation of message formats, routing headers, and rate limits
- Mandatory anti-spoofing controls

5. Micro-Segmentation

- Logical segmentation of interconnect traffic
- Isolation of signaling, media, management, and emergency flows
- Containment of breaches to micro-zones

6. DDoS Mitigation

- Inline DDoS scrubbers at POIs
- AI-driven anomaly detection
- Traffic rate limiting at per-operator and per-service level

7. Continuous Monitoring

- 24x7 SOC monitoring
- Security Information and Event Management (SIEM)
- Real-time alerts to DoT, CERT-In, and operators

5. Key Consumer Benefits

1. Protection Against Fraud

- Prevents CLI spoofing, fake calls, Wangiri fraud, and interconnect bypass.
- Reduces financial loss for consumers and enterprises.

2. Uninterrupted and Reliable Service

- Secure routing protects against mass outages caused by cyberattacks.
- Ensures priority routing for emergency calls.

3. Privacy and Data Protection

- Encryption ensures confidentiality of voice, signaling, and metadata.
- Enhances trust in telecom as a critical public utility.

4. Stable and Affordable Tariffs

- Fraud reduction decreases revenue leakage.
- Minimizes the inflationary cost passed to consumers.

5. Greater Trust in Digital Services

- Secures OTP delivery, digital payments, telemedicine, and online education.
- Builds confidence in India's digital public infrastructure (UPI, NDHM, DigiLocker).

6. Risks and Challenges

1. Cost Implications

- Deployment of firewalls, DDoS scrubbers, PKI infrastructure
- Additional OpEx for monitoring and SOC

2. Increased Complexity

- Coordinating security across multiple operators
- Interoperability across legacy PSTN and modern IP cores
- Skill gaps in cybersecurity practice

3. Potential Latency

- Encryption and DDoS processing may introduce minor delays

These risks are manageable with proper planning and standards-based implementation.

7. Safeguards and Phased Implementation Plan

Phase 1: Foundational Controls (0–12 Months)

- Mutual authentication
- SIP-I firewalling
- TLS/IPsec for signaling
- Basic DDoS protection
- Minimum security SLAs (uptime, response time, breach reporting)

Phase 2: Advanced Controls (12–24 Months)

- Micro-segmentation
- Continuous monitoring and SIEM
- Real-time threat intelligence sharing
- VoLTE/VoNR security hardening

Phase 3: Full Zero-Trust Interconnection (24–36 Months)

- Unified zero-trust policies across operators
- Automated policy enforcement
- End-to-end session-level authentication
- Integrated disaster-recovery security

Recommended Measurable SLAs

- 99.99% protected uptime
- Maximum 5 minutes for interconnect security breach notification
- <200 ms signaling latency post-encryption
- DDoS mitigation within 30 seconds
- Quarterly security audit reports to TRAI/DoT

8. Alignment with International Best Practices

Global regulators and standard bodies mandate similar interconnection security:

- **FCC (USA):** Mandatory STIR/SHAKEN for call authentication
- **Ofcom (UK):** Secure IP interconnection and fraud-mitigation obligations
- **ETSI NFV/5G Security:** Zero-trust, micro-segmentation, encrypted signaling
- **GSMA FS.11/FS.19:** Interconnect security, roaming fraud control
- **BEREC (EU):** Mandatory protection of cross-network signaling

India's adoption of secure interconnection aligns with global norms for critical digital infrastructure.

9. Balanced and Consumer-Centric Conclusion

A secure interconnection framework across PSTN–PSTN, PLMN–PLMN, and PLMN–PSTN is fundamental to:

- safeguarding consumer privacy
- preventing fraud and spoofing
- ensuring continuous and reliable calling
- protecting emergency communications
- stabilizing tariffs by reducing revenue leakage
- maintaining national cybersecurity posture

While implementation requires investment and operational coordination, the long-term benefits—**stronger digital trust, protected consumers, resilient infrastructure, and fair tariffs**—far outweigh the costs.

Mandating security at the interconnection layer is therefore **necessary, forward-looking, and aligned with global best practices**, helping India build a secure, trusted, and consumer-centric digital communication ecosystem.

Q6. (a) Should IP-based interconnection be mandated for new interconnections in the regulatory framework? Kindly justify your response.

(b) Should TSPs be mandated to migrate existing TDM based E1 interconnection to IP-based interconnection within a specified period? If yes, suggest timelines. Kindly justify your response.

Comments :

Yes. IP-based interconnection should be mandated for all *new interconnections* in India's regulatory framework. This shift is essential for reliability, affordability, interoperability, network security, and long-term consumer protection.

1. Rationale: Why Mandating IP-Based Interconnection Is Necessary

1.1 India is transitioning to an All-IP telecom ecosystem

Consumers today increasingly use:

- **VoLTE / VoNR (5G voice)**
- **VoIP and app-based calling**
- **IMS-based services (IP Multimedia Subsystem)**
- **IoT/M2M communication**
- **Cloud-hosted communication platforms**

These services inherently depend on IP. Continuing TDM interconnections for new deployments creates **technical fragmentation, additional cost,** and long-term **inefficiencies**, slowing India's digital transformation.

1.2 Improved Quality of Experience (QoE) for Consumers

IP-based interconnection delivers:

- **HD/Ultra-HD voice and video calling**
- **Lower call drops** through end-to-end packet prioritisation
- **Faster call set-up times** using SIP/IMS
- **Better QoS control** through measurable KPIs

Consumers benefit through **greater reliability** and **consistent quality**, especially as voice migrates to LTE/5G.

1.3 Affordability and economic efficiency

IP interconnection reduces:

- Cost of TDM hardware
- Cross-connection charges
- Power, space, maintenance

Savings can be **passed to consumers** through competitive tariffs and broader coverage.

2. Consumer-centric Benefits of Mandating IP Interconnection

2.1 Interoperability + Digital Inclusion

Mandated IP interconnection ensures:

- Seamless calling between **VoLTE, VoNR, VoIP**, PSTN gateways
- Uniform services irrespective of device, operator, or region
- Smoother transition from 2G/3G shutdowns to full 4G/5G

This protects rural and low-income consumers from quality deterioration during network transitions.

2.2 Strengthening Digital Trust & Security

IP allows modern security frameworks:

- **Secure SIP signaling**
- **TLS/IPSec encryption**
- **Mutual authentication between operators**
- **Zero-trust network segmentation**
- **DDoS detection and mitigation**

This can drastically reduce:

- Call spoofing
- Fraudulent VAS activation
- Spam/robocalling attacks
- Interconnection-borne cyber threats

Consumers gain safer digital communication.

3. Risks and Challenges — and How to Mitigate Them

3.1 Transition cost for operators

Legacy TDM systems are still in service. Migration requires:

- Media gateways
- Security upgrades
- IP-capable interconnection equipment

Mitigation:

Adopt a *phased* and *forward-only* approach:

- Mandate IP *only for new interconnections*
- Allow coexistence with TDM for existing interconnects
- Provide a 24–36 month migration roadmap

3.2 Interoperability issues during migration

Mitigation:

- Mandatory conformance to SIP-IMS standards (3GPP / GSMA IR.95 / IR.65)
- Joint testing and certification mechanisms
- TRAI-mandated common reference configurations

3.3 Cybersecurity risks

Mitigation:

Integrate security from Day-1 (see Section 4).

4. Proposed Future-Ready, Industry-Revolutionary IP Interconnection Framework

A modern IP-interconnection architecture must incorporate:

4.1 SDN/NFV-Enabled Interconnection

- Virtualised SBCs, firewalls, and media gateways
- Dynamic routing of IP traffic through programmable network layers
- Automated failover and congestion control

Benefits:

- Lower capex/opex
- Faster provisioning
- Cloud-ready telecom infrastructure

4.2 Cloud-Native Interconnection Fabric

- Deploy interconnection functions in distributed edge clouds
- Geo-redundant POIs
- Multi-operator interconnection hubs

Benefits:

- Lower latency
- Higher availability
- Support for massive 5G/IoT traffic peaks

4.3 Secure Signalling & Zero-Trust Architecture

- SIP over TLS
- SRTP for secured media
- Zero-trust micro-segmentation
- Continuous anomaly detection

Outcome:

- Protection against signaling storms, spoofing, and cyberattacks

- Strong digital trust for consumers

5. Global Standards & Best Practices

India should align with:

- **3GPP IMS standards (Rel-12 to Rel-18)**
- **GSMA IR.34, IR.65, IR.67, IR.95**
- **ETSI NFV/SDN frameworks**
- **EU All-IP migration policies**
- **US FCC VoIP interconnection norms**

Globally, mandating IP for new interconnections is standard practice because it is **future-proof, secure, and cost-efficient.**

6. Final Justification:

Why Mandating IP-Based Interconnection Protects Consumers?

Mandating IP-based interconnection for *new* interconnections is justified because it:

Directly improves consumer experience

- ✓ Better voice/video quality
- ✓ Lower call drops
- ✓ Faster connectivity
- ✓ Consistent QoS across networks

Reduces costs and promotes affordability

- ✓ Lower network capex/opex
- ✓ Encourages competition
- ✓ Reduces inefficient duplication of TDM infrastructure

Enhances safety and digital trust

- ✓ Modern security standards
- ✓ Protection from fraud, spoofing, and cyberattacks

Supports national digital transformation

- ✓ Enables VoLTE/VoNR, 5G, IoT, cloud services
- ✓ Aligns with BharatNet, India Stack, Digital India goals
- ✓ Ensures long-term resilience and interoperability

Future-proofs India's telecom ecosystem

- ✓ Avoids expensive and disruptive conversions later
- ✓ Keeps India aligned with global best practices

Conclusion

Yes, IP-based interconnection should be mandated for all *new* interconnections.

It is essential for better quality, affordability, reliability, security, and India's long-term digital competitiveness.

A phased, standards-based, secure, SDN/NFV-enabled interconnection framework will ensure that consumers benefit from a truly modern, resilient, and future-ready telecom ecosystem.

(b)

1. Introduction: Why Migration Matters for Consumers

India's digital ecosystem is rapidly transitioning to **VoLTE, VoNR/5G, IoT, machine-to-machine networks, cloud communication, and real-time services** such as video calling, CPaaS platforms, and OTT-integrated voice. In this environment, legacy **TDM-based E1 interconnection** — designed for narrowband, circuit-switched telephony — has become a bottleneck.

A **mandated migration toward fully IP-based interconnection** is essential to ensure India's networks remain **reliable, affordable, interoperable, secure, and future-proof**. Consumers today expect HD call quality, seamless roaming, low latency, and uninterrupted connectivity — all of which require native IP-level interconnection.

2. Why IP-Based Interconnection is Essential for India's Next-Generation Telecom

2.1 Native Compatibility with Modern Technologies

IP interconnection is required for:

- **VoLTE & VoNR (5G voice)**
- **IMS-based call control**
- **5G standalone (SA) architecture**
- **IoT, M2M, and industry automation**
- **Real-time applications (AR/VR, emergency services, telemedicine)**

TDM cannot support these capabilities without complex conversion layers, which increases latency, reduces quality, and raises costs.

2.2 Efficiency and Scalability

IP-based interconnection supports:

- **Flexible bandwidth allocation**
- **Better utilization of transport capacity**
- **Simplified network design**
- **Dynamic scaling for peak loads**

This directly contributes to **lower consumer tariffs**, especially for voice and IoT services, because operators gain efficiency across their transport and interconnection layers.

2.3 Enhanced Consumer Experience

Migration to IP ensures:

- **HD and Ultra-HD voice** (VoLTE/VoNR quality end-to-end)
- **Lower call drops**
- **Faster call setup times**
- **Consistency across networks (fixed, mobile, OTT, enterprise cloud)**

This strengthens consumer confidence and **digital trust** in telecom services.

2.4 Interoperability for a Unified Digital India

IP interconnection allows seamless communication between:

- PSTN ↔ mobile
- LTE ↔ 5G
- Operators ↔ enterprises ↔ CPaaS platforms

- IoT/M2M devices ↔ cloud networks

This accelerates innovation and ensures that **consumers benefit from a unified national communication ecosystem rather than fragmented legacy islands.**

3. Consumer Benefits of Mandated IP Migration

3.1 Improved Quality & Reliability

- Native support for **HD voice, video calling, and real-time multimedia**
- **End-to-end encryption** possibilities
- Lower chances of congestion via dynamic routing

3.2 Affordability

- IP networks are cheaper to scale and maintain
- Savings are passed to consumers in the form of:
 - Lower voice tariffs
 - Affordable enterprise connectivity
 - Cheaper IoT/M2M plans

3.3 Future-Proof Digital Ecosystem

Consumers benefit from:

- Ready availability of 5G services
- Nationwide emergency communication improvements
- Better rural and remote connectivity through flexible IP backhaul options

3.4 Stronger Digital Trust

IP networks support stronger:

- Authentication
- Secure signaling (SIP-TLS, IPsec)
- DDoS protection
- Fraud reduction (CLI spoofing, Wangiri, robocalls)

This protects consumers from scams, spam, and fraudulent calls.

4. Risks & Transition Challenges

4.1 Legacy & Rural Networks

- Some operators, especially in rural areas, still use TDM switches
- Migration may require upgrades in tandem switches, media gateways, and backhaul

4.2 Upfront Capex & Opex

- IMS core expansion
- SBCs, IP-edge security, and QoS implementation
- Training & operational restructuring

4.3 Interoperability During the Transition

Temporary coexistence of IP, VoLTE, VoNR, and TDM may lead to:

- Mixed quality of calls
- Potential signaling translation issues
- Need for synchronization of routing databases

These risks can be fully mitigated with **phased timelines and uniform regulatory oversight**.

5. Proposed Phased Migration Timeline

A realistic, consumer-friendly, multi-stakeholder migration plan is recommended:

Phase 1 (0–12 Months): Mandatory Readiness

- All new interconnections must be **IP-based only**
- Operators must create/upgrade:
 - SIP-based POIs
 - SBCs with standardized security
 - IMS routing framework
- Legacy E1 interconnections to remain operational but not expanded
- Mandatory publication of migration roadmaps by operators

Phase 2 (12–24 Months): Dual Operation with Priority to IP

- At least **50% of all interconnection traffic** must be IP-based
- Inter-operator commercial agreements (RIOs) updated to reflect IP SLAs
- Rural/remote TDM nodes begin progressive migration
- Mandatory QoS standards for IP interconnection:
 - Jitter < 30 ms
 - Packet loss < 0.1%
 - MOS > 4 for HD voice

Phase 3 (24–36 Months): Decommissioning of TDM Interconnection

- All major urban LSAs fully IP-interconnected
- TDM interconnection remains only for remote/rural exceptions with transparent reporting
- No new TDM infrastructure allowed

Phase 4 (36–48 Months): Complete National IP Interconnection

- Nationwide shift to IP-only interconnection
- TDM nodes fully dismantled or isolated
- Unified signaling and security framework established
- Support for **future services (VoNR, RCS, emergency 112 IP calls)**

This phased approach balances **consumer protection**, **operator preparedness**, and **global best practices** seen in countries like the EU, USA, Japan, and South Korea.

6. Alignment with Global Best Practices

Most advanced telecom regulators (FCC, Ofcom, EU BEREC, Japan MIC) mandate full IP interconnection for:

- 5G rollouts
- Universal emergency communication
- Digital identity and secure calling
- Unified licensing regimes

India's transition will ensure:

- Global interoperability
- Compliance with GSMA/ITU standards
- Future readiness for cloud-native telecom

7. Conclusion: Why Mandating IP Migration is Good for Consumers

Mandating migration from TDM-based E1 to IP-based interconnection is essential because it:

- ✓ **Enhances call quality and reduces call drops**
- ✓ **Makes services affordable and future-ready**
- ✓ **Strengthens digital security and trust**
- ✓ **Enables seamless interoperability and innovation**
- ✓ **Aligns India with global 5G and cloud-communication standards**

A phased, regulated, and time-bound mandate ensures that the shift is **orderly, fair to operators, and maximally beneficial to consumers**, while preserving reliability during the transition.

India's telecom future is **IP-native**, and mandated migration is a foundational step toward delivering high-quality, affordable, and secure digital communication for every consumer.

In summary :

Consumer Impact Table for Migration to IP-Based Interconnection

Consumer Dimension	Impact After Migration to IP-Based Interconnection	How Migration Enables It
Call Quality (HD/Ultra HD)	Crystal-clear voice, reduced distortions, natural sound	Native support for HD codecs (AMR-WB, EVS), lower latency, no TDM-IP-TDM conversions

Consumer Dimension	Impact After Migration to IP-Based Interconnection	How Migration Enables It
Call Drops & Reliability	Lower call drops and fewer failed call attempts	Dynamic bandwidth allocation, congestion avoidance, SIP-based signaling pathways
Affordability of Voice & IoT Services	Lower tariffs, cheaper IoT/M2M connectivity, cost-effective enterprise voice	Operators save Opex/Capex with simplified IP networks and pass benefits to consumers
Faster Call Setup Time	Calls connect 30–50% faster	SIP signaling reduces setup delays compared to TDM circuits
Interoperability Across Networks	Seamless calls between VoLTE–5G–Fixed Line–Enterprise CPaaS	Unified IP routing, no dependency on E1 circuits or legacy switches
Digital Trust & Security	Better protection from fraud, spoofing, Wangiri scams, robocalls	End-to-end encryption, SBC-based screening, analytics-driven fraud detection
Improved Rural Connectivity	Stable quality even on mixed networks; faster service rollouts	IP backhaul is cheaper, easier to scale, supports wireless/optical transport
Future-Readiness (5G/IoT/Cloud)	Consumers get access to modern services like VoNR, video calling, cloud communication	IP is the native layer for all next-gen telecom technologies
Emergency Services (112)	Reliable location-sharing, low-latency emergency calling	SIP-based emergency routing, integration with NG-112 systems

Consumer Dimension	Impact After Migration to IP-Based Interconnection	How Migration Enables It
Service Innovation	New digital services, enterprise solutions, and CPaaS/UCaaS offerings	IP allows real-time multimedia, APIs, cloud-native digital frameworks

Comparison Chart — TDM Interconnection vs IP-Based Interconnection

Parameter	TDM-Based E1 Interconnection	IP-Based Interconnection (SIP/IMS)
Technology Base	Circuit-switched	Packet-switched, SIP/IMS-native
Compatibility with 4G/5G/VoLTE/VoNR	Not compatible; requires gateways	Fully compatible; no transcoding required
Call Quality	Limited to narrowband codecs; lower MOS	HD/Ultra-HD voice with AMR-WB/EVS; high MOS
Latency & Call Setup Time	Higher latency due to conversion	Low latency, faster call setup
Scalability	Requires adding physical E1s; limited scalability	Dynamic scaling; bandwidth on demand
Network Efficiency	Inefficient bandwidth utilization	High efficiency via packet routing
Interoperability	Fragmented; operator-specific gateways	Universal—fixed, mobile, enterprise, OTT
Fraud Detection & Security	Minimal inherent security features	Supports encryption, SBC filters, analytics, DPI

Parameter	TDM-Based E1 Interconnection	IP-Based Interconnection (SIP/IMS)
Opex/Capex Requirements	High (TDM switches, E1 cards, hardware maintenance)	Lower long-term costs (software-driven, cloud-ready)
Innovation Readiness	Not suitable for digital services, APIs, or cloud integration	Enables IoT, M2M, CPaaS, UCaaS, RCS, 5G-SA applications
Emergency Services Integration	Limited support for location-based IP emergency routing	Full support for NG-112, location sharing, advanced emergency frameworks
Reliability & Redundancy	Rigid, single-path; expensive redundancy	Multi-path redundancy, dynamic failover via SDN/NFV
Regulatory Fit for Future Telecom	Not aligned to global trends; sunset in most markets	Aligned with global best practices (EU, USA, Japan, Korea)
Consumer Experience	Basic telephony	Rich multimedia, secure, seamless digital communication

Q7. Should the existing processes of ‘provisioning and augmentation of ports at POIs’ under Chapter IV of the TIR 2018 in respect of following need revision: i. ii. iii. Seeking of ports at POIs, Request for initial provisioning of ports, and Request for augmentation of POIs? Kindly provide your response with justification.

Comments :

1. Why Revision Is Necessary for Consumer Protection

The existing processes in **Chapter IV of TIR 2018**—related to (i) seeking ports at POIs, (ii) initial provisioning, and (iii) POI augmentation—were designed in a legacy telecommunication environment primarily dominated by TDM circuits and manual provisioning workflows.

However, **India's telecom ecosystem today is IP-dominated**—5G, VoLTE, VoWiFi, OTT-interworking, enterprise cloud services, and IoT networks require highly dynamic and scalable interconnection.

Consumers ultimately face the consequences of delays or bottlenecks in POI provisioning:

- **Call drops & call failures** during peak periods
- **Poor QoS** in cross-network calls
- **Higher tariffs** due to inefficiencies and congestion
- **Slow resolution timelines** when networks scale rapidly (e.g., during festivals, elections, disasters)

Updating these processes is therefore directly linked to **consumer welfare, affordability, reliability, and digital trust**.

2. Recommendation: The Processes Under TIR 2018 Should Be Revised

Yes, the processes for **seeking ports, initial provisioning, and POI augmentation** should be revised to reflect technological advancements and global best practices. Revised processes should:

- **Reduce time and uncertainty** through automation and API-driven workflows
- **Improve demand forecasting** to prevent congestion

- **Enable cloud-native, software-defined interconnection** that is rapidly scalable
- **Ensure transparent monitoring** via dashboards and real-time analytics
- **Strengthen consumer protections** through strict SLAs

3. Technology Innovations That Can Transform POI Processes

A. API-Driven Automation for Requests & Approvals

- Replace email-based/manual correspondence with secure APIs.
- Enable automated, structured and time-stamped POI requests.
- Auto-verification of utilisation %, traffic patterns, and threshold breaches.

Impact for Consumers:

Faster provisioning → fewer call drops → improved reliability.

B. Cloud-Native & SDN/NFV-Based POIs

- POIs can be virtualised using **Network Function Virtualisation (NFV)**.
- Traffic routing and capacity allocation can be managed dynamically through **Software Defined Networking (SDN)**.
- Virtual POIs reduce dependence on physical ports and speed up capacity scaling.

Impact for Consumers:

Highly stable call experience, lower prices due to reduced OPEX.

C. AI-Based Demand Forecasting

- Predict traffic surges due to festivals, events, new consumer acquisitions, or network expansions.
- Enable **pre-emptive augmentation** rather than reactive provisioning.

Impact for Consumers:

Proactive capacity ensures smooth calling even during peak hours.

D. Real-Time Telemetry & Network Analytics

- End-to-end telemetry from switches, softswitches, IMS nodes, routers, and SBCs.
- Allow real-time utilisation monitoring, with automated alerts when thresholds exceed pre-set values (e.g., 70%, 80%, 90%).

Impact for Consumers:

Transparency and early congestion detection → prevents call failures.

4. Proposed Revisions to the Processes Under TIR 2018

A. Revised Process for Seeking Ports at POIs

1. **Automated API-based request submission**
2. Mandatory submission of:
 - 30-day utilisation report (auto-generated)
 - AI-generated forecast for next 90 days
3. **Real-time acknowledgement** instead of 48 hours
4. **System auto-flags urgency** based on congestion levels
5. All requests visible on a **Central Interconnection Dashboard (CID)** for TRAI

B. Revised Process for Initial Provisioning of Ports

1. Adopt **fully automated port allocation** through NFV/SDN wherever feasible
2. Cloud-native POI instances should be recommended for new deployments
3. Auto-provisioning completed within **T+7 days** instead of current long variability
4. End-to-end provisioning checklist auto-verified through system logs

C. Revised Process for POI Augmentation

1. Utilisation thresholds should trigger **automatic augmentation workflows**:
 - At **70% utilisation** → warning
 - At **80% utilisation** → auto-initiation of augmentation request
 - At **90% utilisation** → mandatory augmentation
2. Virtual POIs allow augmentation in **hours** instead of days/weeks
3. Daily telemetry reports auto-submitted to TRAI
4. Consumer-impact metrics (call failures, congestion rate) must be visible to both operators

5. Proposed Measurable SLAs (for Consumer Protection)

Process	Proposed SLA	Current Pain Point
Acknowledgement of POI request	Instant (API-based)	Manual delays
Initial provisioning of POIs	7 days	Weeks to months
Augmentation decision	48 hours	Uncertain, opaque

Process	Proposed SLA	Current Pain Point
Augmentation implementation	7–10 days (physical) /	
24–48 hrs (virtual)	Long delays causing congestion	
Daily telemetry submission	Automated, continuous	No real-time visibility
Dashboard updates	Every 15 minutes	No public-facing transparency

These SLAs directly benefit consumers by ensuring **fewer call failures, faster expansion, and affordable service quality.**

6. Transparent Governance Model

A **Central Interconnection Dashboard (CID)** hosted under TRAI should include:

A. Operator-facing dashboards

- Real-time utilisation of POIs
- Pending port requests & SLA countdown
- Forecasted congestion zones

B. TRAI-facing dashboards

- Traffic patterns across LSAs
- Compliance with SLAs
- Chronic congestion points

- Penalty triggers for non-compliance

C. Public-facing transparency (high-level)

- Quarterly performance reports
- Average call success rates
- Network reliability indicators

This strengthens **digital trust** and ensures consumer-centric regulation.

7. Risks and Mitigation

A. Interoperability challenges

Mitigation: Common API standards, TRAI technical reference framework.

B. Transition cost for smaller operators

Mitigation:

- TRAI may allow a phased adoption.
- Permit shared cloud-native POIs through neutral host models.

C. Cybersecurity risks with automation

Mitigation:

- Mutual authentication
- Secure encryption
- Zero-trust architecture
- TRAI-certified API standards

D. Resistance to transparency

Mitigation: Mandatory dashboard reporting with penalty framework for non-compliance.

8. Phased Implementation Roadmap (Recommended)

Phase 1 (0–6 months): Standardisation

- Develop TRAI-defined API schemas
- Define telemetry standard
- Publish updated SLAs

Phase 2 (6–18 months): Automation & Dashboards

- Integrate API-based workflows
- Real-time dashboards operational
- Begin virtual POI trials

Phase 3 (18–36 months): Cloud-Native & Predictive Systems

- Full NFV/SDN-ready POIs
- AI-based demand forecasting mandatory
- Public transparency reports released quarterly

Phase 4 (36+ months): Full Modernisation

- Interconnection fully digital, dynamic, elastic
- Industry-wide behavioural change toward proactive expansion

9. Conclusion: Balanced Justification

Updating the TIR 2018 processes for POI port request, provisioning, and augmentation is essential to protect consumers in a rapidly digitising

telecom landscape. Modernisation through **APIs, SDN/NFV, cloud-native POIs, telemetry, and AI forecasting** ensures:

- Fewer call drops
- Better voice and data quality
- Faster scaling of networks
- Lower operational costs → improved affordability
- Transparent governance and digital trust

International practices in the EU, US, Japan, and South Korea demonstrate that **automation-driven interconnection frameworks** significantly improve QoS while reducing complexity.

A revised, tech-enabled Chapter IV under TIR 2018 will therefore **strengthen interoperability, protect consumer rights, and support India’s evolution into a globally competitive digital communications ecosystem.**

Comparison Table: Current TIR 2018 vs Proposed Revised Process

Area	Current TIR 2018 Process	Proposed Revised Process (Future-Ready, Consumer-Centric)
1. Submission of Request for Ports at POI	<ul style="list-style-type: none"> • Mostly manual, email-based requests. • Non-standard formats across operators. • Acknowledgment within 48 hours but often delayed. 	<ul style="list-style-type: none"> • API-based automated submission, with a single digital format defined by TRAI. • Instant auto-acknowledgment (time stamped). • Eliminates delays & subjectivity.
2. Data for Raising POI Request	<ul style="list-style-type: none"> • Manual utilisation reports submitted by operators. • 	<ul style="list-style-type: none"> • Auto-generated utilisation reports from real-time telemetry. •

Area	Current TIR 2018 Process	Proposed Revised Process (Future-Ready, Consumer-Centric)
	Limited cross-verification or analytics.	AI-based 30/90-day forecasts must accompany request. • Full audit trail visible to TRAI.
3. Criteria for Seeking POI Ports	<ul style="list-style-type: none"> • Based primarily on 70% utilisation rule. • Reactive, triggered after congestion starts. 	Predictive and pre-emptive model: • 70% = Warning • 80% = Auto-initiated augmentation workflow • 90% = Mandatory augmentation • AI forecasting prevents congestion before it happens.
4. Initial Provisioning of POIs	<ul style="list-style-type: none"> • Physical ports provisioned manually. • Variation in timelines across circles. • Dependence on hardware availability. 	Cloud-native POIs and SDN/NFV-based provisioning. • Port provisioning automated (where virtual). • SLA: Complete within 7 days (physical) or 24–48 hours (virtual).
5. POI Augmentation Workflow	<ul style="list-style-type: none"> • File-based approvals, manual escalation. • Congestion may continue during processing. 	Automated augmentation workflow triggered by telemetry. • Digital approval flows with SLA countdown clocks visible to both operators and TRAI.
6. Inter-Operator Coordination	<ul style="list-style-type: none"> • Dependence on email, meetings, bilateral communications. 	Secure inter-operator API channel with structured communication. • Logs automatically archived for compliance.

Area	Current TIR 2018 Process	Proposed Revised Process (Future-Ready, Consumer-Centric)
7. Monitoring of POI Utilisation	<ul style="list-style-type: none"> • Periodic reporting (weekly/monthly). • Lag in detection of congestion. 	Real-time telemetry (updated every 15 minutes). • Live congestion alerts sent to operators and TRAI.
8. Governance and Oversight	<ul style="list-style-type: none"> • Limited visibility for TRAI. • No unified data dashboard. 	Central Interconnection Dashboard (CID) maintained by TRAI: • Live utilisation, SLA compliance, pending requests. • Operator comparison panels.
9. Transparency to Consumers	<ul style="list-style-type: none"> • No consumer-facing data. • Call failures not visible publicly. 	Quarterly public transparency reports: • Call success rate • POI congestion trends • Interconnection reliability index
10. SLA Enforcement	<ul style="list-style-type: none"> • SLAs exist but monitoring is manual. • Penalties applied only after prolonged issues. 	Automated SLA tracking and penalty triggers. • Escalation matrix governed by transparent data logs.
11. Scalability of POI Capacity	<ul style="list-style-type: none"> • Physical port-dependent, slow to expand. 	Elastic, cloud-native POIs scale dynamically with demand.
12. Interconnection Architecture	<ul style="list-style-type: none"> • TDM/physical-port centric. 	IP-first, cloud-native, software-defined interconnection with automation and AI.
13. Consumer Impact	<ul style="list-style-type: none"> • Risk of call drops, congestion, and poor quality. • Delays in augmentation → user dissatisfaction. 	Improved QoS: • Fewer call drops • Faster issue resolution • Better voice quality • More affordable tariffs due to reduced OPEX

Area	Current TIR 2018 Process	Proposed Revised Process (Future-Ready, Consumer-Centric)
14. Cost & Efficiency	<ul style="list-style-type: none"> • Higher operational burden on operators. • Manual provisioning increases cost. 	Lower costs due to automation, virtualisation, and predictive scaling. • Efficiency gains passed on to consumers.

Q8. Should the existing framework for Interconnection process and timelines, as provided in the existing TRAI regulations including, The Telecommunication Interconnection Regulations (TIR) 2018, The Telecommunication Interconnection (RIO) Regulations, 2002, and The Telecommunication Interconnection (Charges and Revenue Sharing) Regulation 2001 be revised or continued. Kindly indicate challenges, if any, currently being faced in the implementation of the framework by the TSPs and their possible remedies. Kindly provide your response with detailed justifications.

Comments :

1. India's interconnection ecosystem—guided by **TIR 2018**, **RIO 2002**, and the **2001 Charges & Revenue Sharing framework**—was developed for a telecom environment dominated by TDM switching, predictable traffic, and largely manual provisioning.

Today, consumers rely on:

- **IP-based voice (VoLTE, VoWiFi)**
- **5G SA networks**

- **OTT–telecom interworking**
- **Cloud services, IoT, enterprise connectivity**

The volume, diversity, and dynamism of traffic have fundamentally changed. **The existing regulatory timelines and frameworks can no longer fully protect consumers** against congestion, call failures, or service quality degradation.

Therefore, there is a strong case for **targeted revision**—not abandonment—of the current frameworks to ensure they remain future-ready, consumer-friendly, and innovation-driven.

2. Should the Frameworks Be Revised or Continued?

Balanced Position:

The fundamental principles of TIR 2018, RIO 2002, and the 2001 Charges & Revenue Sharing regulations should continue, but their processes, timelines, and technology standards require significant revision to meet consumers’ expectations of quality, affordability, transparency, and digital trust.

In other words:

Continue the frameworks → Modernise the mechanisms.

3. Consumer-Centric Justification for Revision

A. Quality of Service (QoS) & Reliability

Consumers experience:

- Call drops during congestion

- Low answer-seizure ratios (ASR)
- One-way audio in IP interconnect
- Long delays in resolving interconnection issues

These directly arise from:

- Manual POI provisioning
- No real-time monitoring
- Slow or inconsistent adherence to SLAs

Consumers deserve interconnection that is dynamic, automated, and resilient.

B. Affordability

Delays and inefficient provisioning create:

- Higher OPEX for TSPs
- Sub-optimal routing
- Underutilised or overworked POIs

These translate to higher consumer tariffs or poorer service for the same tariff.

Automated and virtualised interconnection improves efficiency and lowers cost → delivering more affordable telecom service.

C. Transparency & Digital Trust

Consumers have limited visibility into:

- Interconnection congestion

- Call drop causation (device/network/interconnect?)
- Compliance of TSPs with SLAs

A modernised framework with public-facing dashboards increases **trust, accountability, and informed consumer choice**.

4. Current Implementation Challenges Faced by TSPs

1. **Manual and paper/email-based processes** → slow, error-prone, and opaque.
2. **Legacy hardware-dependent POIs** → slow augmentation, costly maintenance.
3. **Multiple bilateral RIOs (2002 model)** → inconsistent formats, interpretation issues.
4. **Static SLAs** → not aligned with dynamic IP-based networks.
5. **Lack of real-time telemetry** → congestion identified only after consumer complaints.
6. **Disputes take weeks/months** to resolve due to lack of shared data.
7. **Uneven implementation** between large and small TSPs.
8. **Security concerns** → signaling attacks, fraud, and spoofing in inter-network paths.
9. **Scaling issues** during sudden traffic spikes (festivals, elections, disasters).
10. **No AI/ML forecasting** → reactive instead of proactive augmentation.

These challenges ultimately degrade **consumer experience** and increase **network costs**.

5. Industry-Revolutionary Technological Remedies

A. API-Based, Automated Interconnection Processes

- Replace emails/letters with secure API channels.
- Auto-validate utilisation, configure ports, update SLAs.
- Machine-readable formats under a TRAI standard.

Consumer benefit: Faster provisioning → fewer call drops.

B. SDN/NFV & Cloud-Native POIs

- Virtual POIs running in cloud or edge DCs.
- Automated scaling based on real-time demand.
- Reduced dependency on physical hardware.

Consumer benefit: Stable service even in peak load.

C. AI/ML-Based Demand Forecasting

- Predict interconnection capacity needs 30/90/180 days ahead.
- Trigger proactive augmentation.

Consumer benefit: Congestion eliminated even before it occurs.

D. Real-Time Telemetry & Autonomous Monitoring

- Continuous monitoring of ASR, congestion, Jitter, MOS, delay, packet loss.
- Alerts at 70/80/90% utilisation thresholds.
- Shared telemetry with TRAI.

Consumer benefit: Higher call quality and faster problem resolution.

E. Zero-Trust Security Architecture

- Mutual authentication between TSP networks.
- Encrypted signaling and data paths.
- DDoS protection at interconnection borders.

Consumer benefit: Protection from spoofing, fraud, and call tampering.

F. Automated Reconciliation for Charges & Revenue Sharing

- Intelligent mediation and automated settlement.
- Common templates to avoid disputes.

Consumer benefit: Reduced cost of interconnect settlement → lower tariffs.

6. Recommended Measurable SLAs (Revised)

Process	Current TIR 2018 / RIO	Proposed SLA
Acknowledgment of POI request	48 hours	Instant API-based
Initial provisioning	~Weeks	7 days (physical) / 24–48 hrs (virtual)
Augmentation decision	10–15 days	48 hours
Augmentation completion	20–30 days	7–10 days (physical) / 24–48 hrs (virtual)
Telemetry submission	Weekly/Monthly	Continuous (every 15 minutes)

Process	Current TIR 2018 / RIO	Proposed SLA
Dispute resolution	Weeks/Months	7-day binding resolution via digital audit logs
Compliance dashboard update	NA	Every 15 minutes

These SLAs ensure **consumer-first outcomes** in quality and affordability.

7. Dispute Resolution Model

A. Data-Driven, Time-Bound, Automated

1. **Digital audit logs** from telemetry + API workflows
2. **Joint access** to TSPs and TRAI
3. Binding resolution in **7 days**
4. Penalty auto-triggered if SLA breached
5. Escalation only for exceptional cases

B. Special treatment for consumer-impacting issues

Congestion affecting >1% of POI traffic must be resolved in **48 hours**.

Consumer benefit: Faster resolution → uninterrupted service.

8. Phased Implementation Roadmap

Phase 1 (0–6 months): Standards & Governance

- Define API schemas, telemetry standards, and security baselines.
- Publish updated SLAs and interconnection templates.

Phase 2 (6–18 months): Automation Rollout

- Deploy API-based workflows across all TSPs.
- Initiate virtual POI pilots in major LSAs.
- Launch TRAI’s Central Interconnection Dashboard.

Phase 3 (18–36 months): Full Modernisation

- SDN/NFV-based interconnection across operators.
- Mandatory AI forecasting.
- Automated revenue sharing and reconciliation.

Phase 4 (36+ months): Consumer Transparency

- Public quarterly reports on interconnection quality.
- Multilingual alerts for outages or interconnect issues.

9. Multilingual Consumer Communication

To enhance transparency and empower all citizens, TSPs should:

- Publish **simple multilingual infographics** explaining congestion, interconnection upgrades, or outages.
- Provide consumer notification in **all 22 scheduled Indian languages** for major disruptions.
- Share quarterly “Network Quality & Interconnection Health Cards” with consumers.

This builds **digital trust**, especially in rural and underserved regions.

10. Conclusion: A Balanced, Consumer-First Position

TRAI's interconnection frameworks (TIR 2018, RIO 2002, and 2001 Charges & Revenue Sharing) should continue as the foundational regulatory structure.

However, their:

- **timelines,**
- **processes,**
- **technological underpinnings,** and
- **transparency requirements**

must be **modernised** to reflect India's IP-driven, 5G-centric, cloud-native telecom future.

A forward-looking and consumer-centric revision—anchored in **automation, virtualization, AI forecasting, zero-trust security, and real-time telemetry**—will ensure:

- Higher call completion
- Lower service costs
- Fewer disputes
- Greater competition
- Stronger digital trust
- Empowered consumers

This balanced approach aligns India's interconnection regime with **global best practices** while protecting the rights and interests of over **1.2 billion telecom consumers**.

Current Interconnection Framework vs. Proposed Modernised Framework

Dimension	Current Framework (TIR 2018, RIO 2002, Charges 2001)	Proposed Modernised, Consumer-Centric Framework
Regulatory Foundation	Based on legacy TDM-era architecture; incremental updates made over time.	Retain foundational principles but overhaul mechanisms to suit IP/5G cloud-native networks.
Process for Seeking POI Ports	Email/manual submission; inconsistent formats; 48-hour acknowledgment.	API-based automated submission with instant acknowledgment; standardised digital templates.
POI Provisioning	Physical, hardware-dependent provisioning; variable timelines.	SDN/NFV-based virtual/elastic POIs; automatic scaling; 24–48 hrs for virtual provisioning.
POI Augmentation Process	Reactive; triggered only after congestion; 15–30 days to complete.	Proactive augmentation: AI-based forecasting + auto-trigger thresholds at 70/80/90%; completion within 7–10 days.
Traffic Monitoring	Weekly or monthly reports; delayed detection; manual verification.	Real-time telemetry updated every 15 minutes; automated congestion alerts; continuous TRAI visibility.
Transparency	Limited operator visibility; no consumer-facing insights.	Central Interconnection Dashboard (CID) for TRAI + quarterly public reports for consumers.
Dispute Resolution	Bilateral negotiation; long timelines	7-day binding, data-driven resolution using API logs, telemetry, and automated audit trails.

Dimension	Current Framework (TIR 2018, RIO 2002, Charges 2001)	Proposed Modernised, Consumer-Centric Framework
	(weeks/months); lack of shared evidence.	
Charges & Revenue Sharing	Manual reconciliation; risk of disputes; delays in settlement.	Automated digital settlement engine , reducing cost and eliminating disputes; transparent reconciliation.
Security Model	Traditional perimeter security; weak against modern threats.	Zero-trust architecture : mutual authentication, encrypted signaling, DDoS protection.
Interconnection Architecture	Physical POIs; fixed-port arrangements; dependent on hardware.	Cloud-native POIs , containerised functions, scalable virtual interconnect edge.
Demand Forecasting	No predictive modelling; dependent on historical utilisation.	AI/ML-based demand forecasting (30/90/180 days) with pre-emptive capacity planning.
Inter-Operator Coordination	Human-driven coordination via emails, meetings, & bilateral agreements.	Automated inter-operator API gateway with end-to-end time-stamped logs and SLA countdowns.
Congestion Management	Congestion addressed after consumer impact; no auto-alerts.	Predictive congestion management via telemetry + AI; actions triggered automatically.
Compliance Monitoring	Manual, periodic verification by TRAI.	Real-time automated compliance checks ; dashboards for TRAI with penalty auto-triggers.

Dimension	Current Framework (TIR 2018, RIO 2002, Charges 2001)	Proposed Modernised, Consumer-Centric Framework
SLA Structure	Static SLAs; loosely enforced; lack of real-time monitoring.	Measurable SLAs with digital tracking: • Instant acknowledgment • 7-day provisioning • 48-hour augmentation decision • 15-minute dashboard updates
Consumer Impact	Call drops, congestion, unpredictable resolution, higher operational costs.	Improved QoS, fewer call drops, faster upgrades, lower costs → better affordability and trust.
Consumer Communication	Technical disclosures only; no multilingual outreach.	Multilingual updates & network health cards explaining outages, upgrades, & interconnect quality.
Interconnection Templates (RIO 2002)	Bilateral, long, inconsistent across TSPs.	Common, standardised, digital RIO templates with machine-readable fields.
Technology Neutrality	Designed primarily for TDM/IP hybrid environment.	Future-ready and tech-agnostic: supports VoLTE, VoWiFi, 5G SA, cloud SBCs, IoT networks.
Flexibility & Scalability	Limited flexibility; capacity increase tied to CAPEX-heavy hardware.	Elastic, cloud-based scaling reduces CAPEX and accelerates response to consumer demand.
Global Benchmarking	Lags behind practices in Japan, EU, USA, and S. Korea.	Aligned with global best practices (automation, virtualisation, zero-trust, AI-driven O&M).

Q9. Whether there is a need to revise the existing process of disconnection of POIs as provided in the regulation 11 of the

Telecommunication Interconnection Regulations (TIR) 2018? If yes, what specific changes should be done in the disconnection procedure? Kindly justify your response.

Comments :

1. Regulation 11 of TIR 2018 establishes the rules for **disconnection of POIs** in cases of non-compliance, non-payment, or breach of interconnection obligations. While the regulatory intent is sound, the current procedure was designed for a **TDM-centric era** with limited automation and asymmetric traffic environments.

In today's India—where consumers depend heavily on **VoLTE, VoWiFi, IP interconnect, 5G SA, OTT interworking, and mission-critical digital services**—POI disconnection, even partial or temporary, can immediately disrupt millions of users.

Therefore, the disconnection framework must be **modernised** to ensure that no consumer suffers from preventable service interruptions.

2. Why Modernisation of POI Disconnection is Necessary for Consumers

A. Protecting Continuity of Service

Abrupt disconnection can cause:

- Call failures between networks
- One-way audio or call setup failures
- Emergency and essential service disruptions
- Consumer panic and loss of trust

Consumers should never be collateral damage in inter-operator disputes.

B. Ensuring Affordability

Weak dispute resolution and sudden disconnections often force operators into:

- Expensive ad-hoc rerouting
- Over-provisioning of emergency capacity
- Higher operational costs that may be passed on to consumers

A predictable and transparent disconnection regime reduces cost volatility.

C. Enhancing Transparency & Digital Trust

Consumers have the right to know:

- Why disruptions occur
- Whether their operator is complying with interconnection rules
- Whether critical POIs are at risk of disconnection

Today, this transparency is missing, leading to consumer confusion.

D. Avoiding Market-Level Disruption

Uncoordinated disconnections:

- Distort competition
- Affect MNP flows
- Create perception of instability in telecom services

A modern, phased, dispute-resolved disconnection framework preserves **market fairness** and **consumer confidence**.

3. Risks in the Current Disconnection Process

1. **Abrupt disconnection risk** due to limited transparency and real-time monitoring.
2. **Consumer impact not explicitly factored** into disconnection timelines.
3. **Manual dispute handling** → long delays, miscommunication.
4. **Lack of redundancy safeguards** before POI shutdown.
5. **TSPs may face hidden costs** due to sudden rerouting or manual provisioning.
6. **No real-time dashboards** for the regulator or public.
7. **Limited guidance on disconnection in an IP/5G environment** (cloud-native IMS, SBCs, SDN/NFV).
8. **Potential impact on emergency, banking, telemedicine, and government services.**

These gaps highlight the need for a reformed, automation-enabled disconnection framework.

4. Industry-Revolutionary Solutions for a Modern Disconnection Framework

A. Automated Real-Time Monitoring of Compliance

- Live telemetry from POIs (congestion, utilisation, signaling errors).
- Automatic detection of non-compliance before it escalates.
- Early warning system triggered at policy-violation thresholds.

Outcome: Prevents disputes from reaching disconnection stage.

B. AI-Driven Dispute Resolution Before Disconnection

- Machine-based comparison of utilisation, payments, port requests, and SLA logs.
- Automated diagnosis of whether the issue is due to misconfiguration, capacity shortage, or policy breach.
- Digital audit logs shared with both TSPs and TRAI.

Outcome: 70–80% disputes resolved without affecting consumers.

C. Phased & Layered Disconnection with Redundancy Protection

Disconnection should never be a single-step action.

Recommended phases:

1. **Phase-0:** Automated early warning
2. **Phase-1:** TRAI-mediated digital dispute resolution
3. **Phase-2:** Partial throttling with informational alerts (no consumer impact)
4. **Phase-3:** Redundant pathways provisioned
5. **Phase-4:** Controlled disconnection with regulator oversight

Outcome: Consumers remain unaffected even during final enforcement.

D. Cloud-Native POI Management

- Virtual POIs allow traffic migration to alternate nodes.
- SDN routing dynamically shifts flows to maintain continuity.
- Zero-touch orchestration ensures faster compliance corrections.

Outcome: Disconnection risk becomes near-zero for consumers.

E. Zero-Trust Security in Disconnection Workflow

- Mutual authentication between operator systems.
- Role-based access for disconnection commands.
- Cryptographically verifiable logs.

Outcome: Prevents misuse, sabotage, or accidental disconnection.

5. Proposed Changes to the POI Disconnection Procedure

A. Mandatory Advance Notice Period with Consumer Safeguards

Replace vague or bilateral timelines with clear regulatory requirements:

- **7-day digital notice to the other TSP** (Phase-1).
- **Simultaneous notice to TRAI** with reasons and telemetry evidence.
- **Consumer impact assessment (CIA)** mandatory before approval.
- **No disconnection** if consumers would suffer due to operator dispute.

B. Redundancy & Continuity Safeguards

Before initiating any disconnection:

- Redundant POIs must be verified as active.
- SDN-based alternative routing configured.
- Virtual POIs pre-provisioned (where feasible).
- Non-disruptive failover tested.

Only after alternate paths are secured should disconnection proceed.

C. Regulator-Controlled Transparency Dashboards

A **TRAIs Central Interconnection Dashboard** should reflect:

- Live POI health
- Pending disputes
- Notices issued
- SLA countdown clocks
- Consumer impact ratings
- Status of redundancy provision

This ensures **trust, accountability, and fairness**.

D. Multi-Level Review Before Disconnection

1. **Operator-to-Operator Review** (automated + bilateral)
2. **TRAI Technical Review** (based on telemetry)
3. **TRAI Consumer Impact Review**
4. **Approval for Phased Disconnection**

Disconnection cannot be unilateral; it must be regulator-approved.

E. Public, Multilingual Communication for Significant Consumer Impact

If disconnection may impact calling:

- Mandatory notice through SMS/IVR in **multiple Indian languages**.
- Simple consumer-facing FAQ: “What is happening? Why? How long?”
- Commitment that no consumer action is required.

This builds **consumer trust and prevents panic**.

6. Revised Disconnection Timeline Framework (Suggested)

Stage	Proposed Timeline	Consumer Safeguard
Early Warning	Immediate (auto-alert)	No impact
Notice Period	7 days	CDR & telemetry review by TRAI
Dispute Resolution	Within 5 days	Automated, data-driven
Redundancy Validation	Within 2 days	Failover tested
Phased Disconnection (if unavoidable)	24–48 hours	Alternate paths active
Final Enforcement	With TRAI approval	Public communication

7. Alignment with Global Best Practices

Countries like **Japan, South Korea, Singapore, the EU, and the US** include:

- Multi-phase disconnection safeguards
- Automated monitoring
- Mandatory redundancy verification
- Regulator-controlled enforcement
- Consumer-first transparency

India can leapfrog these systems by combining SDN/NFV, cloud-native POIs, and AI-driven dispute resolution.

8. Conclusion: A Balanced, Consumer-First Justification

The POI disconnection mechanism should **not merely penalise operators**—it must **protect consumers, ensure continuity, and maintain competitive neutrality**.

A modernised disconnection framework under Regulation 11 of TIR 2018 should therefore be:

- **Consumer-centric**
- **Data-driven**
- **Automated**
- **Transparent**
- **Redundancy-assured**
- **Regulator-supervised**
- **Aligned with global best practices**

With automated monitoring, phased enforcement, real-time dashboards, and cloud-native interconnection, India can ensure **zero consumer disruption**, fair competition, and strong digital trust—even during disputes.

Comparison Table: Current vs Proposed POI Disconnection Process

Dimension	Current Disconnection Process (Reg. 11, TIR 2018)	Proposed Modernised, Consumer-Centric Disconnection Process
Regulatory Basis	Based on legacy TDM-era interconnection and manual compliance checks.	Retain regulation but modernise for IP, VoLTE, VoWiFi, 5G SA, cloud-native interconnects.

Dimension	Current Disconnection Process (Reg. 11, TIR 2018)	Proposed Modernised, Consumer-Centric Disconnection Process
Trigger for Disconnection	Mostly based on disputes (non-payment, non-compliance); often detected late.	Automated early-warning alerts via real-time telemetry before breaches escalate.
Monitoring	Manual, periodic, operator-driven reporting.	Continuous real-time telemetry , auto-flagging violation thresholds (70/80/90%).
Dispute Diagnosis	Human-driven, slow; disagreement on utilisation & compliance data.	AI-driven dispute resolution using time-stamped logs, telemetry, and machine-assisted analysis.
Notice Mechanism	Emails/letters; timelines vary; limited transparency.	Mandatory 7-day digital notice , auto-acknowledged, with simultaneous submission to TRAI.
Transparency to Regulator	Limited, manual exchanges; no shared dashboards.	Central Interconnection Dashboard (CID) for TRAI: real-time POI health, dispute status, SLA timers.
Consumer Safeguards	Not explicitly integrated; consumers often face fallout.	Consumer Impact Assessment (CIA) required before any disconnection; no disconnection allowed if it harms consumers.
Redundancy Requirements	Not mandatory; alternate paths may not exist.	Mandatory redundancy verification : virtual POIs, SDN failover paths, alternative routing validated before any action.

Dimension	Current Disconnection Process (Reg. 11, TIR 2018)	Proposed Modernised, Consumer-Centric Disconnection Process
Phasing of Disconnection	Disconnection can be abrupt if dispute escalates; mostly bilateral.	Five-phase, consumer-safe model: 1) Early Warning 2) Digital Dispute Resolution 3) Controlled Throttling (no consumer impact) 4) Redundancy Activation 5) TRAI-approved Final Disconnection
Role of TRAI	Intervenes when disputes become severe.	Active oversight from early stage: telemetry monitoring, SLA countdowns, pre-disconnection approval.
Operator Coordination	Manual coordination via meetings/emails; prone to disagreement.	API-driven inter-operator communication with cryptographically verifiable logs.
Security	Traditional perimeter controls; risk of accidental/malicious disconnection.	Zero-trust security: role-based access, mutual authentication, encrypted signaling, tamper-proof logs.
Consumer Communication	Not required; consumers remain unaware of disruptions.	Mandatory multilingual consumer alerts (SMS/IVR) for any event with potential consumer impact.
Time Bound Dispute Resolution	Weeks or months.	Binding resolution within 5–7 days via automated audit logs + TRAI review.
Failover Capability	Limited; dependent on physical POIs.	Cloud-native POI management , SDN routing, elastic virtual POIs ensure continuity during disputes.

Dimension	Current Disconnection Process (Reg. 11, TIR 2018)	Proposed Modernised, Consumer-Centric Disconnection Process
Disconnection Execution	Bilateral, sometimes abrupt, limited oversight.	Controlled, regulator-supervised, data-driven disconnection with assured consumer continuity.
Impact on Mission-Critical Services	Risk of outage in banking, telemedicine, emergency calls.	Guaranteed continuity for emergency & critical services through redundancy and phased disconnection.
Consumer Outcomes	Call failures, poor experience, confusion, loss of trust.	Continuity, affordability, transparency, predictability, and strong digital trust.

Q10. Is there a need to introduce a process for the surrender or closure of POIs in the regulatory framework? If yes, what should be the criteria, procedure, charges, and timelines, including the minimum retention period for POIs before a surrender or closure request can be made? Kindly justify your response.

Comments :

Introducing a Process for Surrender or Closure of POIs

1. As India transitions to an **IP-first, 5G-enabled, cloud-native telecom ecosystem**, the management of interconnection infrastructure has become more dynamic. Operators may need to **surrender or close POIs** due to network consolidation, migration to virtual/cloud-native POIs, traffic pattern shifts, or lifecycle upgrades.

However, without a structured regulatory framework, POI closure carries serious risks to **consumer continuity, affordability, transparency, and digital trust**.

A formal, modernised process for POI surrender or closure is therefore essential to safeguard consumers and ensure responsible inter-operator coordination.

2. Why a Structured POI Closure Framework is Essential for Consumer Protection

A. Ensures Continuity of Service

Unregulated or abrupt POI shutdowns may cause:

- Call failures between networks
- Congestion on alternative POIs
- Emergency service disruption
- Poor cross-network voice quality

Consumers must be fully insulated from such risks.

B. Protects Affordability

Unplanned closures increase costs due to:

- Sudden rerouting
- Temporary capacity expansion
- Emergency provisioning

These costs can indirectly affect tariffs if not regulated.

C. Enhances Transparency & Digital Trust

Consumers today expect stable, reliable connectivity.

A transparent process—backed by regulatory oversight—prevents:

- Finger-pointing between operators
- Confusion about service outages
- Loss of consumer confidence in the network

D. Ensures Market Stability

Uncoordinated POI closures may:

- Distort competition
- Affect MNP flows
- Create unfair traffic imbalances
- Disrupt enterprise and OTT traffic partners

A structured framework helps maintain a fair and predictable interconnection ecosystem.

3. Risks of an Unregulated POI Closure Process

1. **Abrupt shutdowns** without preparation or redundancy.
2. **Disputes** regarding utilisation, charges, notice period, or alternate arrangements.
3. **Hidden costs** shifting to consumers or small operators.
4. **Congestion** on remaining POIs due to poorly planned migration.
5. **Poor visibility** for TRAI, leading to delayed intervention.
6. **Negative consumer impact** — call drops, poor quality, and emergency call failures.

The absence of a formal framework makes both consumers and operators vulnerable.

4. Industry-Revolutionary Solutions for Future-Ready POI Closure Management

A. Automated Monitoring of POI Utilisation & Health

- Real-time telemetry across POIs
- Traffic trend analysis
- Automatic flagging of POIs with declining utilisation or underperformance

Outcome: Closure decisions are data-driven, not abrupt.

B. AI-Driven Demand Forecasting

- Predict shifting traffic patterns 30/90/180 days ahead
- Forecast utilisation on alternate POIs
- Identify optimal timing for closure

Outcome: Zero risk of congestion or service degradation during transition.

C. Cloud-Native & Virtual POIs

- Virtual POIs on cloud or edge DCs
- Dynamic capacity scaling
- Ability to gracefully migrate traffic before closure
- Integration with SDN/NFV for automated failover

Outcome: Consumers experience seamless transitions.

D. Redundancy Safeguards

Before surrender/closure:

- Alternate POIs must be ready
- SDN-based routing reconfigured
- Virtual POIs provisioned as backup

Outcome: Network integrity preserved.

5. Proposed Criteria for Allowing POI Surrender/Closure

A. Minimum Retention Period

- A POI must remain operational for **at least 12–24 months** after activation, unless replaced by upgraded/virtual POIs.

B. Utilisation Thresholds

Closure can be considered only if:

- Utilisation is below **30–40%** for a continuous period of **90 days**, OR
- Traffic has shifted to another designated POI as part of planned migration.

C. Redundancy Requirements

Before closure:

- Alternative POIs must have **≥30% spare capacity**
- SDN/NFV routing must be tested
- Virtual POIs provisioned if required
- Emergency call routing validated

D. Consumer Impact Assessment (CIA)

Operator must evaluate and certify that closure will not:

- Increase call drops
- Create congestion
- Affect emergency or banking services
- Harm consumers in rural/remote areas

E. TRAI Approval

Closure should only proceed after:

- All criteria are met
- CIA is submitted
- TRAI verifies redundancy
- A 15-day public disclosure window (via TRAI portal)

6. Recommended Procedure for POI Surrender or Closure

Step 1: Advance Notice

- **90–180 days** prior notice to the interconnecting operator.
- **Simultaneous notice to TRAI** with telemetry and utilisation evidence.

Step 2: Joint Assessment

- Evaluate redundancy, forecast traffic, and consumer impact.
- AI-generated reports to validate utilisation trends.

Step 3: Regulator Review

- TRAI reviews compliance, redundancy, and consumer safeguards.
- TRAI may seek clarifications or mandate additional redundancy.

Step 4: Phased Closure

1. **Phase 0:** Early warning issued
2. **Phase 1:** Traffic migration to alternate POIs
3. **Phase 2:** Parallel operation period (30–60 days)
4. **Phase 3:** Controlled reduction of traffic
5. **Phase 4:** Final shutdown with TRAI approval

Step 5: Validation

- Operator must submit proof of stable traffic on alternate POIs.
- TRAI may run independent QoS checks.

Step 6: Public Transparency

- TRAI publishes POI closure notices on its portal.
- Operators provide multilingual advisory on possible service improvements or routing changes (if any).

7. Recommended Charges Framework

A. Cost Recovery for Operators

- Allowed: recovery of reasonable costs related to migration, testing, and alternate provisioning.
- Not Allowed:
 - Penalty-like charges
 - Charges that increase the burden on small operators

- **Any charge that directly or indirectly burdens consumers**

B. No Consumer Impact

- No tariff change due to POI closure
- No charges for call rerouting
- No change in QoS parameters required from users

8. Recommended Timelines

Stage	Proposed Timeline
Advance Notice	90–180 days
Redundancy Preparation	30–60 days
Parallel Operation	30–45 days
TRAI Review	15 days
Phased Closure	15–30 days
Total Recommended Duration	Minimum 90 days; ideal 180 days

Longer timelines ensure stability, protect consumers, and allow careful technical transition.

9. Alignment with Global Best Practices

Countries such as **Japan, South Korea, the EU, Singapore, and the US** use:

- Multi-stage migration
- Redundancy verification
- Cloud-native interconnects
- Regulator oversight

- Mandatory public notices

India can leapfrog by integrating **automation, AI forecasting, SDN/NFV, virtual POIs**, and real-time dashboards into the closure framework.

10. Conclusion: A Consumer-First Justification

A structured POI surrender/closure process is **essential** to ensure that consumers remain fully protected from service disruptions. The proposed framework:

- Maintains **service continuity**
- Ensures **affordability**
- Enhances **transparency and trust**
- Enables **predictable network evolution**
- Supports India's shift to **cloud-native, automated, IP-first telecom**
- Aligns with **global best practices**

A future-ready framework—rooted in **redundancy safeguards, AI forecasting, automated monitoring, transparent dashboards, phased closure, and regulator oversight**—will guarantee that Indian consumers continue to receive **high-quality, affordable, and reliable connectivity**, even as networks evolve.

Side-by-Side Comparison Table: Current vs Proposed POI Closure Process

Dimension	Current POI Closure Process (Unstructured / Partially Regulated)	Proposed Modernised, Consumer-Centric POI Closure Process
Regulatory Basis	No explicit, detailed framework for POI surrender/closure; handled bilaterally.	Formal TRAI-defined framework with structured procedures, criteria, timelines, and oversight.
Trigger for Closure	Operator-driven decisions; may be based on network consolidation or disputes.	Data-driven triggers: low utilisation trends, migration to cloud-native POIs, planned upgrades.
Monitoring of Utilisation	Manual, reactive, inconsistent across operators.	Automated real-time telemetry with AI/ML-based utilisation & traffic forecasting (30/90/180 days).
Consumer Safeguards	Not explicitly defined; risk of disruption during abrupt closure.	Mandatory Consumer Impact Assessment (CIA) before approval; no closure allowed if service continuity is threatened.
Notice Requirements	No uniform advance notice obligations.	Mandatory 90–180 day advance notice to TSPs and TRAI with utilisation reports & redundancy plan.
Transparency to Regulator	Limited visibility; TRAI informed only after issues arise.	Central Interconnection Dashboard (CID) shows live POI status, utilisation, migration progress, and closure requests.
Redundancy Planning	Not uniformly required; alternate POIs may not be ready.	Mandatory redundancy proof: 30% spare capacity at alternate

Dimension	Current POI Closure Process (Unstructured / Partially Regulated)	Proposed Modernised, Consumer-Centric POI Closure Process
		POIs, SDN failover paths, virtual POIs provisioned.
Traffic Migration	May occur abruptly or partially; prone to congestion.	Structured phased migration (parallel operation, controlled reduction, final shutdown).
Phasing of Closure	Typically one-step, bilateral action.	Five-Phase Closure Model: 1) Early Warning 2) Joint Assessment 3) Parallel Operation 4) Traffic Migration 5) TRAI-approved Closure
Role of AI/Automation	Absent; closure decisions not predictive.	AI-driven demand forecasting , automated monitoring, and digital audit logs for dispute-free closure.
Regulator Approval	Not compulsory; varies by operator agreements.	Mandatory TRAI approval based on utilisation, redundancy, and consumer impact verification.
Operator Coordination	Manual, email-based, slow, and opaque.	API-based inter-operator coordination , real-time logs, cryptographically verifiable data.
Public/Consumer Communication	Not required; consumers unaware of changes.	Mandatory multilingual advisory (SMS/IVR/web) for large-scale closures impacting routing/QoS.
Failover Capability	Depends on physical infrastructure; often inadequate.	Cloud-native POIs , SDN routing, elastic virtual POIs ensure seamless rerouting before shutdown.

Dimension	Current POI Closure Process (Unstructured / Partially Regulated)	Proposed Modernised, Consumer-Centric POI Closure Process
Charges / Cost Recovery	No transparent rule; risk of disputes and cost shifting.	Regulated cost recovery: only reasonable migration-related charges; no cost passed to consumers.
Dispute Handling	Lengthy, bilateral; disagreements over utilisation.	Digital, time-bound (5–7 days) resolution using telemetry, AI-generated utilisation logs, and TRAI mediation.
Consumer Outcomes	Risk of call failures, congestion, reduced QoS, confusion.	Continuity, affordability, transparency, consistency, and strong digital trust.

Q11. In order to safeguard the interest of TSPs arising due to financial obligations of interconnection, is there a requirement for furnishing bank guarantee by one TSP to the other TSP? If yes, please provide the process and methodology for determining the initial bank guarantee amount and any subsequent bank guarantee amount, if required. Kindly justify your response.

Comments : **Yes.**

1. Requirement of Bank Guarantee in a Future-Ready Framework

The requirement for furnishing a Bank Guarantee (BG) between TSPs has historically served as a safeguard to protect against financial risks arising from interconnection obligations. While this requirement remains relevant as a **transitional safeguard**, the evolving telecom landscape—marked by

IP-based interconnection, digital-native architecture, and real-time settlement systems—necessitates a **modernized and adaptive approach**.

Thus, **yes**, a BG may still be required in the short to medium term to safeguard interconnection-related financial obligations. However, both its necessity and its methodology should evolve to reflect technological advancement, industry transformation, and consumer interests.

2. Technological Advancements Justifying a Revised Approach

a. IP-Based Interconnection, 5G, and Upcoming 6G

The migration from TDM to IP-based interconnection and the deployment of 5G and soon 6G networks introduce:

- **Real-time traffic monitoring and analytics**
- **Automated billing and reconciliation systems**
- **Enhanced accuracy in measuring traffic and obligations**

These technological capabilities reduce the financial uncertainty that BGs were originally designed to address.

b. Blockchain and AI-Driven Settlement Systems

Modern settlement technologies allow:

- **Tamper-proof financial ledgers (blockchain)**
- **AI/ML-based prediction of settlement liabilities**
- **Automated anomaly detection and fraud prevention**

This substantially minimizes the need for large, static bank guarantees, because financial exposure becomes **predictive, transparent, and verifiable**.

3. Industry Changes Require Adaptive, Not Rigid, Financial Safeguards

a. Increasing Competition and Entry of Innovative Players

The telecom sector is witnessing:

- New regional operators
- IoT/M2M providers
- Cloud communication platforms
- MVNO-like structures

Rigid, high BG requirements can become barriers to entry and may hinder innovation. An adaptive, proportional BG framework will ensure **fair participation** while still maintaining financial discipline.

b. Cloud-Native and Virtualized Networks (NFV/SDN)

Modern networks allow:

- **Dynamic scaling of interconnection capacity**
- **Software-defined routing and QoS controls**
- **Flexible, elastic interconnection models**

Therefore, financial safeguards must evolve to be **usage-linked, dynamic,** and **responsive**, mirroring the agility of next-generation networks.

4. Consumer Benefits From a Modern BG Methodology

a. Seamless Interconnection Enhances Quality and Trust

Ensuring financially-secure, dispute-free interconnection directly results in:

- Better call completion rates
- Higher quality of service
- Reduced congestion
- Greater reliability

Consumers thereby experience uninterrupted and transparent communication services.

b. Lower Barriers Promote Competition and Affordability

Adopting an updated BG methodology leads to:

- Entry of more innovative or smaller players
- Increased market competition
- More affordable tariffs
- Greater service diversity and innovation

Thus, a future-ready BG mechanism indirectly **maximizes consumer welfare**.

5. Proposed Forward-Looking Methodology for Determining Bank Guarantee

a. Transitional Requirement for Initial BG

During the transition period, an initial BG may continue, but its determination should move away from outdated, port-based approaches.

The quantum of the initial BG should be based on:

1. **Expected interconnection traffic**, using predictive analytics
2. **Historical financial performance and payment regularity**
3. **Real-time usage forecasts and dynamic network load**

This ensures proportionality and fairness.

b. Dynamic Methodology for Subsequent BGs

In a technology-enabled environment, subsequent BGs—if required at all—should be determined using:

- **Automated real-time settlement systems**
- **Periodic reconciliation of interconnection usage charges**
- **Blockchain-based tamper-proof financial records**
- **AI-driven risk scoring and anomaly detection**

Such systems will automatically highlight deviations or pending liabilities, reducing the requirement for high BGs.

c. Evolution Toward Reduced or Sunset BGs

As automated, transparent, and predictive settlement ecosystems mature, the sector may progressively shift to:

- **Smart financial contracts**
- **Automated escrow systems**
- **Usage-based exposure management**

This will naturally reduce the reliance on BGs, leading eventually to a **sunset clause** for static guarantees.

6. Conclusion

Yes, BGs may still be required in the short term as a financial safeguard between TSPs. However, the methodology for determining them must be **forward-looking, technology-aligned, adaptive, and consumer-centric**. A data-driven system that leverages IP-based interconnection, blockchain, AI/ML, and automated settlement will ensure:

- Balanced financial risk management
- Lower market entry barriers
- Enhanced interconnection reliability
- Reduced disputes
- Better consumer outcomes

A modernized, dynamic BG framework will strengthen India's telecom ecosystem, support innovation, and align with global best practices in the era of 5G, 6G, and beyond.

Q12. Should a procedure be established for addressing delays in the payment of interconnection-related charges? If yes, what should be the procedure to address such delays? Kindly provide your response with justification.

Comments :

The issue of delays in payment of interconnection-related charges has significant implications for financial stability, industry fairness, and consumer experience. While a procedure to address such delays is necessary, it should not merely reinforce legacy processes. Instead, it must be **forward-looking**, integrating technological advancements, evolving

industry dynamics, and consumer-centric outcomes to ensure equitable, efficient, and dispute-free interconnection settlements.

1. Technological Advancements Enable a Modernized Settlement Framework

a. Automated Real-Time Settlement Systems

With the sector transitioning to IP-based interconnection, 5G and upcoming 6G readiness, modern networks can support:

- **Real-time automated settlement engines**
- **AI-driven analytics for usage monitoring**
- **Blockchain-based tamper-proof financial ledgers**

These technologies ensure accurate and transparent reconciliation of interconnection usage charges, minimizing the scope for delays.

b. Cloud-Native and Predictive Tools

Cloud-native billing platforms, integrated with virtualized network elements, enable dynamic tracking of actual usage. Predictive algorithms can analyze historical behavior to:

- Anticipate potential delays
- Trigger early alerts
- Enable proactive intervention and dispute avoidance

Thus, technology can shift the system from *delay management* to *delay prevention*.

2. Industry Changes Demand a Flexible and Innovation-Friendly Procedure

a. Increasing Complexity of Interconnection Models

With the arrival of 5G SA networks, satellite communications, IoT/M2M ecosystems, and future 6G architectures, interconnection is becoming:

- Multi-layered
- Real-time
- Data-intensive

This complexity necessitates a **modern settlement mechanism**, not dependent on manual or legacy processes.

b. Entry of New Players and Converging Services

As the telecom ecosystem converges with digital services and new operators enter the market, the procedure must:

- Support innovation
- Maintain a level playing field
- Avoid disproportionate compliance burdens for smaller TSPs

c. Virtualization Through NFV/SDN

The sector's shift toward NFV/SDN and cloud-native interconnection points demands **adaptive and usage-sensitive** procedures rather than rigid enforcement frameworks.

3. Consumer Benefits from a Robust and Timely Settlement Mechanism

A transparent and technology-driven settlement process safeguards consumers by:

a. Ensuring Seamless Connectivity and Call Quality

Timely payments prevent interconnection disputes that often lead to:

- Call drops
- Service disruptions
- Poor QoS

b. Enhancing Consumer Trust and Market Fairness

A predictable and transparent financial settlement environment reduces friction between TSPs and promotes sectoral stability.

c. Enabling Innovation and Competitive Pricing

By reducing manual overheads and dispute-related inefficiencies, TSPs can redirect resources to:

- Network upgrades
- Consumer-centric product innovation
- Better tariffs and improved service diversity

Thus, modernizing settlement procedures directly enhances consumer welfare.

4. Proposed Methodology for Addressing Delays in Interconnection Payments

a. A Phased, Technology-Driven Framework

A strong yet flexible procedure should combine **initial financial safeguards** with **advanced digital settlement mechanisms**.

Phase 1: Transitional Safeguards

- Continue existing safeguards such as **bank guarantees**, but align them with **traffic forecasts and real-time usage**, not static port metrics.

Phase 2: Technology-Integrated Settlement

Over time, shift to:

- Automated, regulator-supervised reconciliation
- Blockchain-based settlement ledgers
- AI-driven predictive tools for risk assessment

b. Mandated Periodic Automated Reconciliation

Introduce mandatory **monthly or quarterly automated reconciliation** through a centralized **digital clearinghouse** supervised by TRAI or DoT.

Such a clearinghouse would:

- Minimize disputes
- Ensure transparency
- Enable neutral and consistent validation
- Maintain a real-time dashboard of obligations and payments

c. Graded Penalty System for Delayed Payments

To ensure fairness and proportionality:

- Impose **graded penalties** based on **duration** and **quantum** of delay.
- Allow flexibility when delays arise from genuine operational challenges or verified technical issues.
- Mandate automated penalty triggers where appropriate, reducing manual intervention.

d. Encouraging Interoperable Digital Payment Channels

Promote adoption of interoperable digital payment systems and automated invoice processing across all TSPs, ensuring:

- Faster settlement
- Reduced human error
- Minimized administrative overhead
- Near real-time visibility of settlement obligations

e. Incentivizing Timely and Early Payments

To foster a culture of financial discipline:

- Provide incentives (e.g., priority dispute handling, marginal credit benefits, or reduced guarantee quantum) for TSPs demonstrating consistent, timely payments.
- Such positive reinforcement can significantly reduce chronic settlement delays.

5. Conclusion

Yes, a procedure is required to address delays in the payment of interconnection-related charges. However, such a procedure must not rely solely on legacy frameworks. It should instead be **dynamic, automated,**

transparent, and technology-enabled, fully leveraging advancements in IP-based networks, AI, blockchain, cloud-native systems, and predictive analytics.

A modern, phased settlement mechanism—supported by graded penalties, automated reconciliation, regulator oversight, and incentives for compliance—will enhance financial stability, encourage innovation, and ultimately deliver better connectivity, reliability, and affordability for consumers.

Comparison Table: Current vs Future Settlement Procedure for Interconnection-Related Charges

Parameter	Current Settlement Procedure	Future Settlement Procedure (Proposed)
1. Settlement Mechanism	Largely manual, periodic reconciliation based on exchanged invoices and bilateral communication.	Fully automated, real-time settlement through digital platforms using AI/ML algorithms and blockchain-based reconciliation.
2. Data Collection & Monitoring	Traffic data captured periodically; delays in validation and mismatch resolution.	Continuous, real-time monitoring using IP-based tools, cloud-native analytics, and automated validation systems.
3. Dispute Resolution	Time-consuming, manual, prone to delays and disagreements over usage and charges.	Automated anomaly detection, tamper-proof distributed ledger, predictive risk identification, faster dispute resolution with minimal manual intervention.
4. Transparency of Records	Multiple data sources, human intervention, risk	Single-source-of-truth ledger (blockchain), transparent,

Parameter	Current Settlement Procedure	Future Settlement Procedure (Proposed)
	of discrepancies and delayed updates.	immutable records accessible to both TSPs and regulator.
5. Risk of Delays in Payments	High probability due to manual processes, invoice disputes, and procedural bottlenecks.	Significantly reduced due to automated reconciliation, digital payment systems, and predictive alerts for potential defaults.
6. Financial Safeguards (Bank Guarantees)	Static port-based BG assessment; often disproportionate to actual usage or risk.	Dynamic, usage-based BG linked to real-time traffic forecasts; eventual transition to smart contracts/automated escrow mechanisms.
7. Regulatory Oversight	Fragmented visibility; reliance on post-facto reporting and operator submissions.	Unified regulator-supervised digital clearinghouse offering real-time dashboards and automated compliance tracking.
8. Inclusion of New/WBE/Small Operators	Burdensome compliance; high BG and manual processes may hinder entry of smaller TSPs.	Innovation-friendly, flexible safeguards; reduced entry barriers through automated systems and proportionate settlement obligations.
9. Interconnection Infrastructure	TDM-era processes, limited adaptability, static configurations.	IP-based, virtualized (NFV/SDN), cloud-native interconnection enabling scalable and dynamic settlement frameworks.
10. Consumer Impact	Risk of service disruption due to disputes or delayed payments; lower quality of service.	Seamless connectivity, reduced disputes, higher reliability, better call quality, and greater consumer trust.

Parameter	Current Settlement Procedure	Future Settlement Procedure (Proposed)
11. Payment Method	Manual or batch-process payments, dependent on human intervention.	Interoperable digital payment systems with auto-debit, scheduled smart settlements, and minimal manual handling.
12. Overall Efficiency	Moderate to low; prone to delays and inaccuracies.	High efficiency; automated, accurate, real-time, transparent, and consumer-centric.

Q13. Is there a need to revise the financial disincentive framework as provided in these regulations. If yes, what specific changes should be done? Kindly justify your response. A.2. The Short Message Services (SMS) Termination Charges Regulations, 2013

Comments : **Yes.**

1. Justification for Revising the Framework

The current financial disincentive framework, rooted in the SMS ecosystem of 2013, has become outdated due to fundamental shifts in technology, industry models, and consumer behaviour. Revising it is critical for three reasons:

- To align with **emerging technologies** like RCS (Rich Communication Services), AI, and blockchain
- To reflect **industry shifts** from traditional SMS to OTT messaging ecosystems
- To protect **consumer interest** through better affordability, reduced spam, and improved service reliability

A modernized framework must be **outcome-based, technology-driven,** and **consumer-focused**—ensuring fairness, accountability, and deterrence against abuse.

2. Technology Advancements Necessitate Modern Disincentives

a. Rise of OTT and RCS Messaging

- SMS traffic is declining, replaced by **WhatsApp, Telegram, Signal, and RCS.**
- Business messaging is increasingly shifting to cloud-based, encrypted, feature-rich platforms.

Implication: The disincentive framework must shift from **volume-centric** to **impact-centric**—penalizing disruptive or harmful behavior, not mere volumes.

b. AI-Driven Fraud Detection

- AI/ML can now detect:
 - SMS pattern anomalies
 - Flash flooding
 - Spoofing and phishing attempts

These tools enable **real-time enforcement** and **graduated deterrence** rather than blanket penalties.

c. Blockchain for Audit and Settlement

- Blockchain ensures **tamper-proof SMS delivery records**, allowing transparent and accountable tracking of terminations and failures.

3. Industry Changes Demand a New Regulatory Mindset

a. Decline of Traditional SMS and Rise of Digital Platforms

- SMS is now largely used for **A2P (Application-to-Person)** or **enterprise messages**, not personal communication.
- Business models are evolving with **API-based delivery**, dynamic routing, and **cloud messaging aggregators**.

Implication: The framework must target abuse within **A2P enterprise messaging**, rather than applying outdated peer-to-peer norms.

b. New TSP Business Models

- Many small/new TSPs focus on **termination services, bulk SMS, or reseller routes**.
- Without proper disincentive alignment, it creates asymmetric risks and encourages **spam monetization**.

4. Consumer Benefits from a Revised Framework

- **Spam and fraud prevention:** Consumers are frequently targeted by phishing, fake links, and unsolicited messages.
- **Service reliability:** Delayed or dropped OTPs cause frustration and financial loss.
- **Affordability and trust:** Penalties for abusive practices reduce systemic inefficiencies and increase platform integrity.

A revised framework thus **directly benefits end users**—especially in an era of digital transactions, e-governance, and real-time identity verification.

5. Proposed Changes to the Disincentive Framework

Current Practice	Proposed Future Framework
Fixed penalties per violation (e.g., per unsolicited SMS)	Outcome-based penalties: e.g., per confirmed spam instance, per delayed OTP, per fraud pattern.
Manual, report-based enforcement	AI-driven fraud detection and real-time pattern alerts using ML algorithms.
Uniform penalties for all players	Risk-weighted disincentives: higher penalties for repeat offenders, lower for verified low-risk TSPs.
No direct consumer protection linkage	Consumer impact mapping: disincentives tied to number of affected users or verified consumer complaints.
Minimal deterrence for spoofing/phishing	Severe penalties for fraud: including license suspension triggers, public blacklisting, and telecom ombudsman intervention.

6. Suggested Methodology for Implementation

a. Phased Rollout

- **Phase 1** (Year 1): Continue existing framework with added AI-based spam monitoring by TSPs.
- **Phase 2** (Year 2): Introduce pilot **Regulatory Dashboard** to track performance, spam rates, fraud incidents.
- **Phase 3** (Year 3): Full shift to **graded and dynamic disincentives** based on automated quality-of-service metrics and real-time fraud logs.

b. Regulator-Supervised Dashboards

- TRAI may implement **central dashboards** aggregating:

- Spam rates per TSP
- Fraud complaints (linked to DoT & cybercrime platforms)
- Delayed delivery logs (especially for OTPs)

c. AI-Based Monitoring Standards

- Define regulatory-grade AI standards for:
 - Anomaly detection
 - Sender score reputation
 - Predictive modeling for bulk traffic fraud

This should be **open, auditable, and privacy-respecting**.

d. Multilingual Consumer Alerts and Complaint Tools

- Enable **real-time complaint registration** via SMS/chatbot/web portal in **multiple Indian languages**.
- Alerts for suspected fraud SMS, number blacklists, and verified sender indicators.

7. Conclusion: Towards a Consumer-Protective, Future-Ready Messaging Ecosystem

The SMS Termination Disincentive Framework of 2013 served its purpose in an era where SMS was dominant. But in the **2025 ecosystem of encrypted OTT platforms, cloud messaging APIs, AI fraud detection, and decentralized routing**, we require an **adaptive, intelligent, and consumer-first framework**.

A modernized disincentive system will:

- Protect consumers from spam, fraud, and disruption
- Promote fairness and accountability in A2P traffic
- Incentivize quality over volume
- Foster global best practices for digital trust

We strongly recommend that TRAI adopt a **phased, AI-enabled, outcome-based disincentive model** for SMS termination that truly reflects the digital future of Indian telecom and consumer empowerment.

Q14. Is there a need to revise the existing SMS termination charge? If yes, what are the considerations necessitating such a revision? If not, kindly provide justification.

Comments : **Yes.**

Need for Revising SMS Termination Charges in a Future-Ready, Consumer-Centric Framework :

The telecom messaging ecosystem has undergone a profound transformation since SMS termination charges were originally defined. With the rapid evolution of technology, new digital business models, and heightened consumer expectations for secure and reliable communication, the current SMS termination charge framework requires a comprehensive revision. A future-ready approach must reflect **technological progress, industry restructuring, and consumer protection imperatives.**

1. Technology Advancements Necessitate a Revised Charge Framework

a. Emergence of OTT Messaging and RCS

The explosion of **OTT messaging platforms** (WhatsApp, Signal, Telegram) and the adoption of **Rich Communication Services (RCS)** have altered the economics of messaging. Consumers now use encrypted, feature-rich platforms for most personal communication, reducing pressure on SMS but increasing expectations of reliability for OTP, banking alerts, e-governance messages, and emergency notifications.

b. AI-Driven Fraud Detection and Cloud-Native Routing

Modern networks are capable of:

- **AI/ML-based spam detection**
- **Predictive anomaly detection** in A2P traffic
- **Cloud-native routing** and hyperscale SMS delivery
- **Blockchain-based audit trails** improving message integrity

These capabilities enable **high accuracy, lower fraud rates, and reduced delivery failures**, which should be incentivized through a modernized termination charge model.

c. IP-Based and Virtualized Infrastructure

SDN/NFV and IP-based interconnection allow:

- More efficient routing
- Real-time delivery insights
- Lower operational costs

A legacy cost-plus termination charge no longer aligns with digital-native network environments.

2. Industry Changes Demand Modernization

a. Decline of P2P SMS

Peer-to-peer SMS volumes have steadily declined due to OTT adoption. SMS today is primarily used for:

- **A2P enterprise messaging**
- **Financial OTPs**
- **Government notifications**
- **Emergency alerts**

The charge structure must therefore reflect the economics of **enterprise-grade, mission-critical messaging**, not P2P volumes of the past.

b. Rise of A2P & New Digital Business Models

Enterprises now rely on:

- API-driven messaging gateways
- Cloud communication platforms
- CPaaS (Communication Platform as a Service)

These ecosystems require **predictable, fair, and fraud-resistant termination charges**, ensuring innovation is not hindered by outdated cost assumptions.

c. Increasing Spam, Fraud, and Phishing Threats

Fraudulent SMS traffic, phishing links, header spoofing, and unregistered content have grown significantly. A revised charge system can:

- Penalize abusive routing
- Discourage grey-route traffic
- Reward trusted and verified senders

This shift is essential for consumer safety and digital transaction confidence.

3. Consumer Benefits from Revising SMS Termination Charges

A modernized charge framework directly strengthens consumer trust by delivering:

a. Affordability

Fair termination charges reduce enterprise communication costs, which in turn lowers consumer-facing service fees—especially for banking, OTP-based services, and e-governance.

b. Reliability of Critical Messages

A transparent and incentivised system ensures:

- Faster delivery of OTPs
- Timely banking alerts
- Reliable e-governance messages
- Higher delivery success rates

c. Protection from Spam and Fraud

Charges linked to spam, grey-route misuse, or fraudulent activity promote responsible routing and discourage malicious actors.

d. Trust in Digital Services

Consumers depend on SMS for:

- Aadhaar OTP
- UPI
- Banking transactions
- Health & transport authentication
- Emergency notifications

A future-ready charge framework enhances trust in these vital services.

4. Proposed Methodology for Future-Ready SMS Termination Charges

a. Phased Implementation Framework

1. Phase 1 – Stabilization:

- Continue existing charges with improved spam reporting and mandatory AI-based monitoring by TSPs.

2. Phase 2 – Modernization:

- Introduce outcome-based metrics tied to delivery success, spam incidence, and fraud prevention.

3. Phase 3 – Intelligent Termination Charge System:

- Fully dynamic system using AI/ML analytics and real-time dashboards.

b. Outcome-Based Termination Charges

Instead of fixed per-SMS charges, adopt parameters such as:

- Delivery latency

- Delivery success rate
- Spam/fraud flagging rate
- Sender reputation score
- Route integrity rating

This aligns financial incentives with **quality and consumer safety**, not message volume.

c. Regulator-Supervised Digital Dashboards

TRAI may establish a unified dashboard displaying:

- Real-time SMS delivery rates
- Fraud attempts and blocked traffic
- Spam complaint heatmaps
- Sender ID reputation scores
- Inter-TSP termination metrics

Such dashboards ensure **neutral oversight, transparency, and rapid dispute resolution**.

d. AI-Based Monitoring and Enforcement

Mandate AI tools for:

- Pattern detection
- Grey-route identification
- Content spoofing analysis
- Real-time header misuse detection

Penalties or higher termination charges may apply for repeated non-compliance.

e. Multilingual Consumer Communication

Consumers must receive:

- Fraud alerts in regional languages
- Easy reporting mechanisms (SMS/IVR/app)
- Header verification information
- Simple instructions for phishing avoidance

This strengthens digital literacy and safety across all demographics.

5. Conclusion: A Global Best Practice Model for Consumer Protection

Revising the SMS termination charge framework is essential to align India's messaging ecosystem with global best practices. Leading markets (EU, Singapore, South Korea) are shifting toward:

- **Outcome-based quality charges**
- **AI-enabled fraud detection systems**
- **Cloud-native routing standards**
- **Consumer protection-first frameworks**

India must adopt a **future-ready, tech-enabled, consumer-centric** approach that:

- Ensures affordability
- Secures message integrity
- Protects consumers from fraud

- Supports innovation in enterprise messaging
- Strengthens trust in digital transactions

A revised, intelligent termination charge model will ensure SMS continues to serve as a reliable backbone for India’s digital economy—especially for authentication, governance, banking, and essential citizen services.

Comparison Table: Current vs Proposed SMS Termination Charge Framework

Parameter	Current SMS Termination Framework	Proposed Future-Ready Framework
1. Basis of Charges	Fixed per-SMS termination charge, largely volume-driven and based on legacy cost models.	Outcome-based and dynamic charges linked to delivery success, fraud prevention, latency, and sender reputation.
2. Technology Integration	Minimal use of advanced technologies; manual or batch processing for spam checks.	Use of AI/ML, RCS, blockchain, cloud-native routing , and real-time fraud detection to ensure accuracy and integrity.
3. Traffic Type Consideration	Assumes traditional P2P messaging volumes; uniform approach across traffic types.	Tailored for A2P/enterprise traffic , mission-critical OTPs, and differentiated routing profiles.
4. Fraud & Spam Deterrence	Limited disincentive mechanisms; reactive penalties for unsolicited SMS.	Active deterrence: penalties for spam/phishing, grey-route usage, spoofing; predictive analytics for early detection.
5. Delivery Performance	No direct linkage between termination charges and	Performance-linked charges: lower charges for high QoS; higher

Parameter	Current SMS Termination Framework	Proposed Future-Ready Framework
	quality of delivery (latency, success rate).	for poor delivery or repeated failures.
6. Sender Identity & Verification	Basic alphanumeric header rules, limited penalties for misuse.	Verified sender ecosystem with header reputation scoring , blockchain audit trail, and penalties for misuse.
7. Network Architecture	Designed around legacy SMSC infrastructure; limited support for IP-native messaging.	Cloud-native, virtualized routing (NFV/SDN), integration with RCS and next-gen communication platforms.
8. Regulatory Oversight	Post-facto reporting, manual audits, and periodic compliance checks.	Real-time regulatory dashboards showing delivery KPIs, fraud incidents, spam heatmaps, and inter-TSP metrics.
9. Consumer Protection	Limited focus on consumer harm; spam/fraud addressed mainly through complaint-based action.	Strong consumer-centric model: proactive fraud blocking, multilingual alerts, and guaranteed timely delivery of critical messages.
10. Market Dynamics Consideration	Ignores changing market structure—decline of P2P SMS and rise of enterprise APIs.	Reflects A2P dominance, digital platforms, and CPaaS ecosystems , ensuring fair and competitive pricing.
11. Cost Efficiency	Opaque cost components; often misaligned with real operational expenditure.	Transparent, data-driven cost models using automated settlement, real-time routing analytics, and audit logs.

Parameter	Current SMS Termination Framework	Proposed Future-Ready Framework
12. Incentive Structure	Uniform charges irrespective of quality or compliance.	Incentives for compliant, high-quality SMS delivery ; penalties for fraud, failure, or repeated consumer harm.
13. Global Alignment	Based on outdated regulatory philosophy; diverges from markets adopting AI-driven, outcome-based frameworks.	Harmonized with global best practices (EU, Singapore, South Korea) emphasizing trust, QoS, and fraud prevention.
14. Consumer Impact	Risk of delayed OTPs, increased spam, inconsistent delivery quality.	Reliable, fast, secure OTPs and alerts; reduced spam and fraud; improved trust in digital services.

Q15. Is there a need to prescribe SMS carriage charges when an NLDO carries SMS between the LSAs? If yes, what principles and methodology should apply? If not, kindly provide justification. A.3. Intelligent Network Services in Multi-Operator and Multi-Network Scenario Regulations, 2006.

Comments :

The question of whether SMS carriage charges should be prescribed when National Long-Distance Operators (NLDOs) carry SMS between Licensed Service Areas (LSAs) must be evaluated in the context of the **rapidly evolving digital communication ecosystem**. Traditional SMS carriage models were designed for a voice-centric era; however, India's messaging environment is now shaped by **IP-based networks, AI-driven routing, OTT platforms, and cloud-native interconnects**. A revisited framework must

therefore be **fair, transparent, adaptive, and strongly aligned with consumer protection.**

1. Technology Advancements Demand a Modern Approach to SMS Carriage Charges

a. Rise of OTT Platforms and RCS

OTT messaging (WhatsApp, Telegram, Signal) and RCS messaging have significantly reduced P2P SMS traffic. SMS today is primarily used for:

- **A2P enterprise communication**
- **Real-time authentication (OTP)**
- **Financial transactions**
- **Government notifications**

This change requires carriage charges to reflect **mission-critical, enterprise-driven** SMS use, not legacy personal messaging.

b. AI-Driven Routing and Cloud-Native Interconnects

Modern NLDO infrastructure can now use:

- **AI-based routing optimization**
- **Cloud-native interconnects**
- **Virtualized SMSCs (NFV/SDN)**
- **Blockchain-based message traceability**

These technologies lower operational costs and improve routing efficiency—making it feasible to adopt **cost-based, outcome-oriented carriage charges.**

c. IP-Based Evolution of Long-Distance Transport

With 5G SA and upcoming 6G architectures:

- SMS packets are transported over **IP fabrics**
- Routing becomes more efficient and predictable
- Costs decline due to virtualization and automation

Therefore, carriage charge models must shift from **TDM-era assumptions** to **IP-native realities**.

2. Industry Changes Require a New Charging Philosophy

a. Decline of P2P SMS

P2P SMS has declined sharply in India. Charging mechanisms based on traditional volumes no longer reflect market realities.

b. Rise of A2P and Enterprise Messaging

Enterprises, banks, fintech platforms, OTTs, and government agencies use SMS for secure communication. This ecosystem requires:

- Fair and predictable pricing
- High-quality, low-latency delivery
- Fraud-resistant architecture

Carriage charges must therefore support **trusted enterprise messaging**, not inflate operational costs.

c. New Digital Business Models

CPaaS platforms and cloud-based API messaging gateways dominate the A2P market. Charging should:

- Encourage innovation
- Prevent artificial cost inflation
- Promote interoperability and reliability

A modern framework will ensure India remains a global leader in enterprise messaging.

3. Consumer Benefits from a Rationalized, Future-Ready SMS Carriage Charge Framework

a. Affordability

Cost-efficient carriage ensures lower SMS termination costs for enterprises, which ultimately reduces consumer-facing charges for banking, UPI, ticketing, healthcare, and government services.

b. Reliability of Critical Messages

Consumers depend on SMS for:

- OTP verification
- Banking alerts
- Insurance claims
- Emergency warnings
- Health and vaccination messages

Rational carriage charges incentivize high-quality delivery without congestion or artificial delays.

c. Protection from Spam and Fraud

A well-designed carriage regime supports:

- Real-time anomaly detection
- Anti-spoofing checks
- Prevention of grey-route exploitation

This ensures stronger consumer safety.

d. Trust in Digital Ecosystems

Consumers increasingly rely on SMS to authenticate every major digital transaction. A stable, fair, and efficient carriage system enhances trust in India's digital economy.

4. Proposed Methodology for Determining SMS Carriage Charges for NLDOs

a. Adopt Cost-Based, Technology-Neutral Principles

Charges should be:

- Cost-based
- Proportional to network usage
- Reflective of modern IP transport costs
- Neutral to technology (TDM or IP, SMSC or RCS gateway)

This prevents distortion of competition and eliminates legacy inefficiencies.

b. Introduce Outcome-Based QoS Metrics

Charging should incentivize performance, such as:

- Delivery success rates
- Delivery latency
- Fraud/spam detection success
- Route integrity and security
- Verified sender compliance

This aligns financial incentives with consumer experience.

c. Use Regulator-Supervised Dashboards

Implement TRAI dashboards enabling:

- Real-time monitoring of inter-LSA SMS flows
- Fraud and spam heatmaps
- KPIs linked to routing performance
- Transparent tracking of NLDO-level performance

Dashboards ensure:

- Consumer-centric oversight
- Neutral auditing
- Fast dispute resolution

d. Phased Rollout Approach

Phase 1 – Stabilization (Short Term)

- Continue current mechanisms while collecting granular inter-LSA SMS flow data.
- Mandate AI-based spam monitoring by NLDOs and TSPs.

Phase 2 – Cost-Based Recalibration (Medium Term)

- Introduce rational, cost-based carriage charges aligned with IP-native economics.

Phase 3 – Intelligent Dynamic Charging (Long Term)

- Adopt outcome-based carriage charges that reward performance and discourage misuse.
- Integrate RCS and next-gen messaging into the same framework.

e. Multilingual Consumer Communication

- Provide fraud alerts and SMS authentication education in all Indian languages.
- Encourage simple and accessible reporting mechanisms for spam or suspected fraud.
- Issue periodic advisories from TRAI and TSPs to ensure consumer awareness.

5. Conclusion: Aligning with Global Best Practices and Consumer Protection

Countries transitioning to next-generation messaging ecosystems (EU, South Korea, UAE, Singapore) have adopted:

- Cost-based carriage
- Outcome-oriented QoS-driven charges
- AI-enabled fraud mitigation
- IP-native routing standards

India must now move in the same direction.

A **consumer-centric and future-ready SMS carriage charge framework** will:

- Ensure reliable and secure delivery of critical messages
- Prevent artificial cost escalation
- Foster innovation in enterprise messaging
- Protect consumers from fraud and spam
- Strengthen trust in the digital ecosystem

Prescribing modern SMS carriage charges when NLDOs carry messages between LSAs is not just an economic decision—it is a **consumer protection imperative** and a critical enabler of India’s digital future.

Comparison Table: Current vs Proposed SMS Carriage Framework

Parameter	Current SMS Carriage Framework	Proposed Future-Ready SMS Carriage Framework
1. Charging Principle	No dedicated or standardized SMS carriage charge for NLDOs; based on legacy voice-era assumptions.	Cost-based, transparent, and technology-neutral SMS carriage charges reflecting IP-based transport economics.
2. Traffic Type Assumption	Framework assumes traditional P2P SMS flows and limited A2P movement across LSAs.	Designed for A2P/enterprise-driven traffic , critical OTPs, banking alerts, and government services across LSAs.
3. Technology Basis	Built on legacy TDM/SMSC infrastructure with limited modernization.	Cloud-native routing, AI-driven optimization, IP-based interconnects, RCS integration,

Parameter	Current SMS Carriage Framework	Proposed Future-Ready SMS Carriage Framework
		and virtualized transport layers (NFV/SDN).
4. Cost Drivers	High-cost assumptions from legacy networks; static and unrelated to modern routing efficiencies.	Real-time cost modeling using automated routing analytics, lower IP transport costs, and virtualized infrastructure.
5. Fraud & Spam Controls	Limited visibility; reactive handling of spoofing, phishing, and grey-route exploitation.	AI/ML-driven fraud detection , blockchain audit trails, compulsory header verification, and penalties for misuse.
6. Routing Efficiency	Manual or semi-automated routing; limited use of intelligent algorithms.	AI-powered routing with predictive load balancing, latency optimization, and proactive congestion control.
7. Quality of Service (QoS)	No linkage between carriage cost and quality metrics (latency, success rate).	Outcome-based carriage charges tied to delivery time, success rates, spam mitigation, and route integrity.
8. Regulatory Oversight	Post-facto reporting and manual audits; fragmented visibility across LSAs.	Real-time regulator dashboards showing inter-LSA SMS flows, fraud incidences, routing KPIs, and NLDO performance.
9. Market Dynamics Consideration	Ignores shift from P2P to enterprise A2P messaging; based on outdated traffic trends.	Fully aligns with CPaaS, enterprise API messaging, fintech , and e-governance messaging ecosystems.

Parameter	Current SMS Carriage Framework	Proposed Future-Ready SMS Carriage Framework
10. Incentive Structure	No systematic incentives for reliability, security, or consumer safety.	Incentives for high-quality, secure, low-latency delivery; penalties for fraud, spam, or grey-route leakages.
11. Interoperability	Minimal integration with next-gen messaging standards.	Seamless interoperability with RCS, IP messaging gateways, 5G core, and future 6G communication models.
12. Consumer Protection	Consumer interest addressed indirectly through spam control rules; no linkage with carriage mechanism.	Strong consumer-centric model ensuring affordability, faster OTPs, fewer spam/fraud messages, and higher trust in digital transactions.
13. Operational Transparency	Limited transparency in routing logs and message traceability.	Blockchain-based traceability, real-time routing logs, and tamper-proof delivery confirmations.
14. Global Alignment	Diverges from emerging global norms emphasizing AI-driven, outcome-based, IP-native carriage.	Harmonized with best practices in EU, Singapore, UAE, South Korea, focusing on QoS, fraud prevention, and consumer safety.

Q16. Is there a need to revise the existing access charge to be paid by the service provider to the originating provider for IN services? If yes, kindly provide detailed explanation; if not, kindly provide justification.

Comments : **Yes.**

Revisiting Access Charges for Intelligent Network (IN) Services: A Consumer-Centric, Future-Ready Approach

1. Background and Rationale

The existing Access Charge framework governing payments from the service provider to the originating provider for Intelligent Network (IN) services was established during the era of **legacy circuit-switched networks, SS7 signaling, and hardware-based IN nodes**.

However, the telecom ecosystem has undergone a foundational transformation. **Cloud-native IN platforms, API-driven triggers, IMS/SIP-based service invocation, real-time analytics, and AI-supported fraud control** have reshaped both the cost structure and functional importance of IN services.

Simultaneously, the **consumer journey has shifted** from voice-centric services to **digital, OTT-enabled, enterprise, and IoT-centric workflows**, many of which rely on lightweight IN or IN-equivalent triggers for authentication, routing, and identity assurance.

The legacy Access Charge structure no longer reflects this technological or economic reality. A **review is necessary** not merely for commercial rationalization but to ensure **consumer affordability, reliability, transparency, and safety** in a rapidly digitizing economy.

2. Key Technological Advancements Necessitating Change

2.1 Cloud-Native IN and Virtualization

Modern IN platforms operate on **virtualized, elastic architectures**, drastically reducing CAPEX and OPEX relative to hardware-centric SCP/SSP deployments.

Cost per trigger is now aligned to API usage and compute cycles rather than dedicated switching capacity.

2.2 API-Driven and Modular Service Exposure

Operators now expose IN functionality through **API gateways and service exposure frameworks**, enabling:

- missed-call based authentication,
- toll-free access,
- enterprise-grade service requests,
- real-time digital verification.

The unit cost of service invocation is significantly lower and more predictable.

2.3 IMS/CAMEL Over IP and VoLTE/5G Integration

Migration to **IMS, SIP, and DIAMETER signaling** reduces signaling costs and improves reliability. Many IN features are now delivered as **software-defined, cloud-hosted functions** integrated with VoLTE/5G service layers.

2.4 AI-Driven Fraud Mitigation

Security and consumer protection now depend on **AI-based anomaly detection, real-time scoring, and anti-spoofing tools**.

The Access Charge structure should incentivize operators to deploy and continuously update such systems.

Conclusion:

The technology landscape has shifted from circuit-based triggers to **software-defined, cloud-native, and AI-supported service invocation**, rendering the legacy Access Charge framework obsolete.

3. Industry Trends Influencing Cost and Usage

3.1 Decline of Legacy IN and Rise of Digital/OTT Workflows

Consumers increasingly engage through digital interfaces—apps, portals, wallets—reducing dependence on legacy IN while creating new service-trigger requirements.

3.2 Increased A2P/Enterprise Trigger Usage

Banks, fintech companies, e-commerce platforms, government portals, and emergency systems rely on:

- toll-free IN calls
- missed-call triggers
- verification flows
- enterprise routing requests

The traffic profile is now **enterprise-heavy**, with lower cost per event but higher volumes.

3.3 Emergence of 5G, IoT, and Low-Latency Use-Cases

Next-generation services—IoT telemetry, emergency routing, URLLC service assurance—require **lightweight, rapid, and cost-efficient triggers** incompatible with legacy cost assumptions.

Conclusion:

The access charge must reflect the economic shift from **low-volume, high-cost legacy triggers** to **high-volume, low-cost digital triggers**.

4. Consumer Impact: Why Revising Access Charges Matters

4.1 Affordability

Rationalizing Access Charges lowers costs for:

- toll-free access to citizen services,
- enterprise customer support,
- bank and financial verification flows,
- emergency and grievance channels.

Consumers ultimately benefit from more affordable and accessible services.

4.2 Reliability and Service Continuity

A modernized charging framework encourages investment in:

- resilient cloud-native platforms,
- redundant architectures,
- low-latency response systems.

This ensures **uninterrupted access** to high-impact services.

4.3 Transparency

Predictable, cost-based Access Charges enable:

- clearer tariffs,

- fair cost allocation,
- lesser disputes between operators,
improving consumer trust.

4.4 Safety and Fraud Protection

Linking charges with fraud-control capability encourages deployment of:

- AI-based anomaly detection,
- secure signaling,
- anti-spoofing layers,
- authentication enhancements.

This reduces fraud risk for consumers in critical services (banking, government, helplines).

5. Proposed Implementation Methodology

5.1 Cost-Based Pricing Model

A revised Access Charge should be grounded in:

- updated cost models reflecting **virtualized networks**,
- incremental cost of **API-triggered events**,
- security/fraud management cost components,
- reduced CAPEX/OPEX from IP-based systems.

This ensures rationality, fairness, and transparency.

5.2 QoS and Outcome-Linked Incentives

Introduce **performance-based modifiers**, such as incentives for:

- high service uptime,
- low latency,
- strong fraud prevention scores,
- low consumer complaint rates.

This shifts the framework from **volume-based** to **quality-based** regulation.

5.3 Phased Rollout (36-Month Window)

- **Phase 1 (0–6 months):** Stakeholder consultations, revised definitions, collection of cost data.
- **Phase 2 (6–18 months):** Optional migration for legacy networks, mandatory for new IP-based IN systems.
- **Phase 3 (18–36 months):** Full migration, enforcement of QoS metrics, annual audits.

This avoids market disruption and ensures smooth adoption.

5.4 Regulatory Dashboards for Monitoring

TRAI may establish a real-time dashboard showing:

- IN performance statistics,
- uptime and latency data,
- access charge trends,
- fraud mitigation indicators.

This green-lights transparency and accountability.

5.5 Multilingual Consumer Communication

Public advisories, FAQs, and awareness campaigns in **all major Indian languages** should clarify:

- consumer rights,
- cost implications (if any),
- benefits of modern IN systems,
- protection against fraudulent or spoofed IN calls.

6. Global Best Practices and Justification

Countries with advanced digital ecosystems—EU nations, Japan, Singapore, and South Korea—have adopted **cloud-native service logic, API-based charging, zero-trust security principles, and performance-linked pricing** for service invocation.

India’s revision should align with these standards to:

- promote competitiveness,
- ensure fair cost distribution,
- encourage investment in futuristic digital services,
- protect consumers from fraud, service outages, and exploitative pricing.

7. Policy Recommendation (Summary)

The existing Access Charge framework for IN services should be revised because it:

- is based on outdated legacy costing,
- does not reflect cloud-native architecture,
- fails to incentivize fraud protection,

- imposes unnecessary costs that ultimately affect consumers,
- is misaligned with digital-era and 5G/IoT service requirements.

A modern, cost-based, performance-linked, transparent, and phased implementation approach will:

- **lower consumer costs,**
- **increase reliability,**
- **strengthen digital trust,**
- **promote fair competition,**
- **align India with global telecom best practices.**

**Comparison Table: Current vs Proposed Access Charge
Framework for IN Services**

Parameter	Current Framework (Legacy)	Proposed Framework (Future-Ready, Consumer-Centric)
1. Technology Basis	Built around legacy SS7 / TDM , circuit-switched IN (SCP–SSP).	Based on cloud-native IN , virtualization (NFV), IMS/SIP, DIAMETER, and API-driven triggers.
2. Platform Architecture	Hardware-bound service control points; fixed capacity.	Elastic, virtualized, scalable compute; dynamic resource allocation.

Parameter	Current Framework (Legacy)	Proposed Framework (Future-Ready, Consumer-Centric)
3. Cost Structure	High CAPEX/OPEX due to dedicated nodes, SS7 signaling costs, and maintenance-heavy systems.	Lower, granular, compute-based cost model with reduced overhead and optimized resource use.
4. Unit Cost Per Trigger/Event	Derived from legacy switching and signaling load.	Based on API call cost , compute cycles, cloud utilization, and security processing.
5. Traffic Profile Considered	Voice-centric; low volume, operator-controlled triggers.	Digital, enterprise-heavy , high-volume, A2P/missed-call/verification flows.
6. Treatment of Digital/OTT Services	Not accounted for; originally designed for basic IN services.	Fully compatible with OTT, digital banking, authentication , and 5G/IOT workflows requiring rapid triggers.
7. Support for 5G/VoLTE/IoT Use-Cases	Not aligned with IP-based service invocation.	Optimized for low-latency , IP-native, 5G and IoT-enabled triggers.
8. Fraud & Security Consideration	Minimal; based on static controls.	Linked with AI-based fraud detection , spoofing

Parameter	Current Framework (Legacy)	Proposed Framework (Future-Ready, Consumer-Centric)
		prevention, anomaly scoring.
9. Incentives for Innovation	None; charges based on static historical models.	Incentives for cloud- native upgrades , strong QoS performance, adoption of advanced fraud control.
10. Charging Principle	Volume-based, legacy per-event logic.	Cost-based , future- aligned, modular pricing reflecting cloud/IP economics.
11. Quality of Service (QoS)	No linkage between charges and service uptime/latency.	Outcome-based incentives tied to uptime, low latency, consumer complaint levels.
12. Transparency	Limited; few public disclosures and no standard definitions.	Regulator dashboard , standardized definitions, performance transparency.
13. Consumer Impact on Affordability	Higher operational costs eventually passed to consumers.	Lower cost structure enables affordable toll- free calls, banking

Parameter	Current Framework (Legacy)	Proposed Framework (Future-Ready, Consumer-Centric)
		verification, helplines, etc.
14. Consumer Impact on Reliability	Legacy nodes at risk of congestion and outages.	Cloud-native redundancy ensures continuous, reliable access to critical services.
15. Consumer Protection (Fraud/Spoofing)	Weak; limited tools for protecting consumers from IN-based fraud.	Incentivizes strong AI fraud control , reducing scam, spoofing, and abuse incidents.
16. Alignment with Global Best Practices	Out of sync with modern regulatory benchmarks.	Aligned with EU, Japan, Singapore, South Korea : cloud-native charging and security-linked incentives.
17. Administrative Burden	Higher due to manual processes and outdated architecture.	Lower; automated monitoring , cloud analytics, API logs.
18. Implementation Model	Static, no defined timeline for evolution.	Phased migration (consultation → optional IP pathways → full rollout).
19. Flexibility for Future Services	Low flexibility for digital- first ecosystems.	High adaptability for emerging digital ,

Parameter	Current Framework (Legacy)	Proposed Framework (Future-Ready, Consumer-Centric)
		enterprise, IoT, and AI-driven services.
20. Overall Consumer Benefit	Limited affordability, weak transparency, lower protection.	Strong improvements in affordability, reliability, transparency, and fraud protection.

Q17. Are there any difficulties that service providers encounter in complying with existing IN Regulations, 2006 in Multi-Operator and Multi-Network Scenario? Kindly describe these challenges in detail and suggest possible regulatory remedial measures to overcome these challenges. A.4. TRAI (Transit Charges for BSNL's Cell One Terminating Traffic) Regulations, 2005

Comments :

1. The Intelligent Network (IN) Regulations, 2006 were framed during an era dominated by **legacy circuit-switched networks, SS7 signaling, and hardware-based service control points (SCP)**. Today's telecom ecosystem is drastically different—multi-operator, multi-network, cloud-native, 4G/VoLTE-driven, and rapidly transitioning to **5G, IoT, and digital platforms**.

As a result, service providers face **significant compliance challenges** in applying the 2006 framework to modern architectures. These challenges not

only affect operators but also impact **consumer affordability, reliability, transparency, and digital safety.**

2. Detailed Challenges in Multi-Operator, Multi-Network Scenarios

2.1 Interoperability Issues Across Heterogenous Networks

- Operators use different **IN platforms (legacy SCPs, virtualized SCPs, cloud-native service layers).**
- Interoperability between legacy SS7-based triggers and IP-based CAMEL/IMS triggers is inconsistent.
- Variations in **trigger mapping, routing logic**, and feature sets lead to service fragmentation.

This results in call failures, inconsistent service experience, or delays in service invocation, ultimately affecting consumers.

2.2 Legacy IN Trigger Complexity

- IN Regulations, 2006 were built around **legacy triggers (INAP, CAMEL Phase 1/2).**
- Modern digital services rely on **API-based triggers, microservices, and software-defined logic**, which are **not addressed in the current regulation.**
- Operators struggle to maintain legacy IN logic solely for compliance purposes, increasing costs and operational complexity.

2.3 Billing Disputes and Reconciliation Problems

- Multi-operator IN interactions generate:
 - different event records (IN CDRs, API logs, SIP logs),

- inconsistent timestamping,
 - varied charging granularity.
- This leads to frequent **interconnect billing disputes, delayed reconciliation, and revenue uncertainty.**
- Compliance becomes difficult when service invocation logic varies by network generation (2G/3G vs 4G/VoLTE vs IP).

2.4 QoS Monitoring Limitations

- QoS obligations designed for circuit-switched networks do not reflect:
 - cloud-native latency,
 - dynamic routing,
 - failover times in virtualized environments.
- Traditional KPIs cannot measure modern IN performance, resulting in **compliance ambiguity** and **inadequate consumer protection metrics.**

2.5 Higher Risk of Fraud, Spam, and Spoofing

- Multi-operator IN workflows create **vulnerabilities across signaling boundaries.**
- Legacy IN systems lack:
 - AI-based anomaly detection,
 - spoofing prevention,
 - real-time scoring models.
- Fraud often originates through inconsistent IN triggers across operators, exposing consumers to **VAS fraud, spoofed helpline calls, and identity misuse.**

2.6 Difficulty Integrating Modern Digital/OTT Journeys

- OTT applications use **webhooks, APIs, and digital workflows** not contemplated in 2006 regulations.
- Operators must maintain parallel systems (legacy IN + modern platforms), creating inefficiencies and compliance difficulties.

3. Technology Advancements That Enable a New Approach

3.1 Cloud-Native IN Architectures

- Virtualized SCPs, microservices, and elastic provisioning reduce costs and streamline orchestration.
- Allow standardized, low-latency, more predictable service invocation.

3.2 API-Driven Service Orchestration

- API gateways and open service exposure frameworks support:
 - missed-call triggers,
 - number portability workflows,
 - banking/verification calls,
 - enterprise A2P flows.
- These enable a **simpler, more interoperable alternative** to legacy IN signaling.

3.3 AI-Based Fraud Detection

- Real-time anomaly scoring, spam detection, spoof prevention, and subscriber-level risk analytics protect consumers from IN-based fraud.

3.4 SDN/NFV for Routing and Trigger Management

- Software-defined networking allows dynamic routing, consistent feature invocation, and automated failover across multi-operator networks.

3.5 IMS/CAMEL Over IP

- Move to IP-native signaling aligns better with cloud-native triggers and digital orchestration.

4. Industry Changes Creating New Challenges

4.1 Migration from Legacy IN to Digital/OTT Platforms

- Many consumer services (activation, verification, grievance redressal) now occur through **apps, portals, and digital platforms**.
- Maintaining legacy IN solely for compliance adds cost without consumer benefit.

4.2 Rise of A2P and Enterprise Trigger-Based Workflows

- Banks, government agencies, e-commerce, and fintech platforms generate high-volume **IN/A2P traffic**.
- The 2006 model does not reflect this shift to large-scale enterprise usage.

4.3 Growth of 5G, IoT, and M2M Services

- 5G-enabled workflows require:
 - ultra-low-latency triggers,
 - dynamic resource allocation,

- machine-triggered events.
- These cannot be effectively supported under a legacy IN regulation.

5. Consumer Benefits of a Revised Approach

5.1 Affordability

- Reducing dependence on legacy IN reduces operational costs, enabling operators to offer more affordable toll-free services, verifications, and helplines.

5.2 Reliability

- Cloud-native and SDN/NFV-based workflows offer:
 - better uptime,
 - reduced call failures,
 - consistent triggers across networks.

Consumers experience smoother, more dependable services.

5.3 Transparency

- Standardized APIs and logs create clear audit trails that reduce disputes and increase trust.
- Consumers benefit from transparent pricing and clear service invocation behavior.

5.4 Protection

- AI-enabled fraud detection strengthens consumer safety from spoofing, VAS fraud, and misuse across operator boundaries.

6. Proposed Methodology for Implementation

6.1 Standardized APIs Across Operators

- Define a **unified API schema** for service invocation (toll-free, verification, A2P flows).
- Reduce reliance on legacy INAP/CAMEL variations across operators.

6.2 Outcome-Based QoS Metrics

Revise QoS obligations to measure:

- latency of service trigger execution,
- successful invocation rates,
- failover efficiency,
- AI-based fraud detection performance,
- consumer complaint levels.

6.3 Regulator Dashboards for Transparency

TRAI may host live dashboards on:

- IN performance across operators,
- uptime and latency,
- fraud events prevented,
- QoS compliance,
- billing dispute resolution timelines.

6.4 Phased Rollout

Phase 1 (0–6 months)

- Stakeholder consultation; standard definitions; technical interoperability groups.

Phase 2 (6–12 months)

- Adoption of standardized APIs; optional upgrades for legacy IN.

Phase 3 (12–24 months)

- Mandatory compliance with outcome-based QoS; cloud-native triggers for new services.

6.5 Multilingual Consumer Communication

- Public advisories in all major Indian languages explaining:
 - improved reliability,
 - reduced fraud risk,
 - consumer rights under new frameworks,
 - grievance redressal avenues.

7. Conclusion: Alignment with Global Best Practices and Consumer Protection

Countries with advanced digital ecosystems (EU, Singapore, South Korea, Japan) have moved away from rigid legacy IN frameworks toward **cloud-native service orchestration, secure API-based triggers, fraud-resilient signaling, and performance-linked regulatory regimes.**

Modernizing the IN compliance framework in India is **essential for:**

- Reducing consumer costs,
- Improving reliability and QoS,
- Enhancing digital trust,

- Supporting next-generation services (5G, IoT, fintech, public utilities),
- Strengthening fraud/spam protection,
- Ensuring interoperability across multi-operator environments.

Thus, revising the IN Regulations, 2006 with a future-ready, consumer-centric, interoperable, and technology-aligned approach is both justified and urgently required to safeguard consumer interests and support India’s digital transformation.

**Comparison Table: Current vs Proposed IN Compliance Framework
(Multi-Operator & Multi-Network Context)**

Parameter	Current IN Compliance Framework (Legacy, IN Regulations 2006)	Proposed Future-Ready IN Compliance Framework (Consumer-Centric, Digital-Era)
1. Technology Architecture	Legacy SCP–SSP , SS7/TDM-based networks.	Cloud-native IN , virtualized nodes, microservices, IMS/SIP-based service logic.
2. Trigger Mechanism	INAP/CAMEL Phase 1/2 triggers tied to circuit-switched events.	API-driven service orchestration , webhooks, digital triggers supporting modern workflows.
3. Multi-Operator Interoperability	Fragmented; operator-specific IN variations; inconsistent trigger mapping.	Standardized APIs and schemas , common trigger definitions across operators.
4. Multi-Network Interoperability	Designed mainly for 2G/3G; challenges across	Fully compatible with VoLTE, 5G, IoT, URLLC , and cloud-native routing.

Parameter	Current IN Compliance Framework (Legacy, IN Regulations 2006)	Proposed Future-Ready IN Compliance Framework (Consumer-Centric, Digital-Era)
	4G/VoLTE/IMS and 5G networks.	
5. Service Invocation Consistency	High variation between operators; call failures, inconsistent user experience.	Unified invocation logic ensuring consistent user experience across networks.
6. Billing & Reconciliation	Complex; multiple event record formats (IN CDR, signaling logs) cause disputes.	Unified, API-based logs , timestamp harmonization, automated reconciliation.
7. Fraud & Spam Protection	Basic; depends on static rules; easily bypassed across networks.	AI-driven fraud detection , spoofing prevention, anomaly scoring, signaling integrity.
8. QoS Monitoring	Legacy KPIs not suited for IP/cloud; compliance difficult to measure objectively.	Outcome-based QoS metrics : latency, invocation success rate, failover efficiency, complaint scores.
9. Consumer Transparency	Limited; consumers unaware of IN failures or inconsistencies.	Audit-friendly logs, regulator dashboards , multilingual consumer advisories.
10. Support for Digital & OTT Services	No provisions; built for voice-centric legacy services.	Supports digital banking, eKYC, ecommerce verification, OTT flows , API-first approach.
11. Enterprise & A2P Use-Cases	Not explicitly addressed; legacy IN strained under enterprise loads.	Optimized for A2P, enterprise triggers, toll-free, verification flows .

Parameter	Current IN Compliance Framework (Legacy, IN Regulations 2006)	Proposed Future-Ready IN Compliance Framework (Consumer-Centric, Digital-Era)
12. Cost Structure	High OPEX/CAPEX due to hardware-bound IN nodes.	Lower, compute-based cost model aligned with cloud-native economics.
13. Dispute Resolution	Frequent disputes due to mismatched IN triggers, logs, and definitions.	Standardized event formats , automated log comparison, regulator oversight.
14. Network Evolution Readiness	Not aligned with SDN, NFV, cloud routing, or service exposure architecture.	Fully compatible with SDN/NFV , dynamic routing, cloud-native analytics.
15. Compliance Burden	High—operators maintain legacy systems solely for regulatory compliance.	Lower—modern regulation aligned with operational reality; reduced duplication .
16. Scalability	Limited scalability; vertical scaling of legacy IN platforms.	Elastic, horizontal scaling on virtualized/cloud-native infrastructure.
17. Consumer Affordability	Higher operator costs eventually passed to consumers.	Lower operational cost → more affordable toll-free, banking, helpline services .
18. Consumer Reliability	Call drops, trigger failures across networks reduce service reliability.	Consistent, redundant, low-latency service invocation improves reliability.
19. Consumer Protection	Limited protection from spoofing, VAS fraud, identity misuse.	Enhanced protection via AI-based risk scoring , cross-operator fraud analytics.

Parameter	Current IN Compliance Framework (Legacy, IN Regulations 2006)	Proposed Future-Ready IN Compliance Framework (Consumer-Centric, Digital-Era)
20. Global Best Practice Alignment	Outdated compared to EU, Singapore, South Korea standards.	Aligns with global digital-era standards : cloud-native regulation, secure APIs, zero-trust principles.
21. Regulatory Monitoring	Manual, limited real-time visibility.	Live regulator dashboards , automated monitoring, standardized reporting.
22. Implementation Model	Static regulations with no evolution path.	Phased rollout , flexibility for legacy networks, mandatory compliance for new services.
23. Consumer Impact Summary	Higher costs, inconsistent experience, lower transparency & weaker protection.	Improved affordability, reliability, transparency, and digital safety .

Q18. Is there a need to revise the Telecom Regulatory Authority of India (Transit Charges for Bharat Sanchar Nigam Limited's CellOne Terminating Traffic) Regulation, 2005? Kindly provide your response with justification. A.5. The Telecommunication Interconnection Usage Charges Regulations, 2003.

Comments :

1. The **Transit Charge framework for BSNL's CellOne terminating traffic**, established under the 2005 regulation and aligned with the 2003 IUC regime,

was designed in an era dominated by **TDM-based switching, SS7 signaling, and traditional voice-centric traffic patterns.**

Today, the telecom ecosystem has transformed fundamentally:

- **IP-based interconnection**, VoLTE, and IMS networks are the norm.
- Telecom traffic is increasingly **enterprise, A2P, data-driven, and OTT-integrated.**
- Consumers rely on digital services, not just basic voice.
- Networks are cloud-native, automated, and AI-assisted.

As a result, relying on a **2005-era transit charging model** imposes inefficiencies, creates cost misalignments, and risks consumer disadvantage.

A revised framework—cost-reflective, technology-neutral, future-ready, and consumer-centric—is therefore essential.

2. Why the Current Transit Charge Framework Needs Revision

2.1 Technology Advancements

2.1.1 Migration to IP-Based Interconnection

- Operators increasingly use **SIP, DIAMETER, IMS**, and cloud-native STPs.
- Transit functions now occur over **packet-switched networks**, not circuit-switched TDM trunks.
- The cost profile has shifted from time-based resource occupation to **bandwidth, compute, and routing logic.**

2.1.2 Cloud-Native Routing

- Transit functions today are automated through:
 - SDN/NFV,
 - dynamic path optimization,
 - multi-cloud routing.
- These systems are more efficient, elastic, and lower-cost.

2.1.3 AI-Driven Traffic Management

Modern networks use AI for:

- predictive congestion avoidance,
- fraudulent traffic detection,
- optimized routing decisions.

These reduce operational costs and improve service reliability, implying that legacy per-minute transit costs are no longer representative.

2.1.4 5G/IoT Service Evolution

- Transit traffic increasingly includes **machine-to-machine (M2M)**, low-latency interactions, and service-based routing.
- Legacy TDM-based transit charges do not capture the economics of these modern flows.

Conclusion:

The technological foundation underlying the 2005 transit charges no longer exists in the current IP-native telecom environment.

3. Industry Changes Necessitating Revision

3.1 Decline of Traditional Voice and SMS

- Voice minutes and SMS volumes have sharply declined due to VoIP, RCS, and OTT messaging.
- The original cost drivers for transit charges have diminished.

3.2 Rise of Enterprise, A2P, and OTT Traffic

- Traffic is increasingly **platform-led** (e-commerce, fintech, government services).
- These flows require efficient, low-cost IP-based transit—misaligned with legacy TDM-based charges.

3.3 New Business Models

- Digital services rely on affordable routing for verifications, customer support, toll-free access, and grievance redressal.
- Outdated transit charges create cost distortions that may be passed on to enterprises and ultimately **consumers**.

3.4 Industry-Wide Migration to IP, IMS, and Cloud

- Almost all private operators have migrated to IP-based interconnect.
- BSNL itself is modernizing under **4G/5G revitalization programs**, making the legacy framework obsolete.

4. Consumer Benefits of Revising Transit Charges

4.1 Affordability

Reducing outdated TDM-based transit charges lowers costs for:

- customer care numbers,
- banking verifications,
- government helplines,
- OTT-linked service calls.

The savings ultimately benefit consumers.

4.2 Reliability

IP-based transit routing reduces:

- call drops,
- congestion,
- transit delay.

A modern charge regime incentivizes operators to strengthen high-quality interconnection.

4.3 Transparency

A clear, uniform, cost-based model ensures:

- predictable billing,
 - reduced disputes,
 - simple regulatory oversight,
- benefiting consumers who rely on fair, transparent telecom services.

4.4 Protection from Hidden Costs and Fraud

- AI-driven transit routing reduces spam and fraudulent call rerouting.
- Lower costs reduce incentives for arbitrage-based abuses.

- Consumers see improved protection from spoofed calls and deceptive service charges.

5. Proposed Methodology for Implementing a Revised Transit Charge Framework

5.1 Cost-Based Charging Principles

A modern transit charge model should:

- reflect **actual IP-based resource usage** (compute, bandwidth, routing logic),
- incorporate benefits of **cloud-native efficiencies**,
- be periodically reviewed through transparent cost studies.

This ensures fair pricing, efficient resource use, and affordability for end consumers.

5.2 Outcome-Linked QoS Metrics

Introduce QoS metrics tied to transit charge compliance:

- call completion rate,
- latency,
- jitter in IP-based transit,
- fraud detection effectiveness,
- consumer complaint levels.

Performance-linked incentives ensure operators invest in high-quality interconnection.

5.3 Regulator Dashboards

TRAI can develop a real-time dashboard tracking:

- transit performance metrics,
- interconnection uptime,
- fraud events detected/prevented,
- operator compliance levels.

This enhances transparency and consumer trust.

5.4 Phased Rollout

To ensure minimal disruption:

Phase 1 (0–6 months)

Stakeholder consultation, unified definitions, cost data collection.

Phase 2 (6–12 months)

Optional migration for legacy networks, mandatory for new IP-based networks.

Phase 3 (12–24 months)

Full adoption of revised transit charges, integrated with IP-based routing and outcome-based QoS.

5.5 Multilingual Consumer Communication

Publish consumer advisories in all major Indian languages explaining:

- the purpose of revised transit charges,
- benefits (better reliability, lower costs),

- grievance and redressal mechanisms.

This ensures inclusivity and awareness.

6. Conclusion: Alignment with Global Best Practices and Consumer Protection

Advanced digital economies (EU, Singapore, South Korea, Japan) have moved away from per-minute TDM-era transit regimes toward **IP-based, cloud-native, cost-reflective, interoperability-focused frameworks**.

Revising the 2005 CellOne Transit Charge regulation is essential for India because it:

- ensures **consumer affordability**,
- strengthens **network reliability**,
- enhances **transparency and fraud protection**,
- supports the digital ecosystem (fintech, ecommerce, government services),
- aligns interconnection economics with IP, VoLTE, and 5G architectures,
- reduces disputes and simplifies regulatory oversight.

A modern, consumer-centric, technology-neutral transit charging framework is crucial for India’s transition toward a secure, efficient, next-generation telecom ecosystem—fully aligned with global best practices and national digital priorities.

Comparison Table: Current vs Proposed Transit Charge Framework

Parameter	Current Transit Charge Framework (2005, TDM-Era)	Proposed Future-Ready Transit Charge Framework (IP-Based, Consumer-Centric)
1. Technology Basis	Based on TDM, SS7, circuit switching , and fixed trunk groups.	Based on IP-based interconnection , SIP/IMS routing, cloud-native transit.
2. Network Architecture	Centralized, hardware-based switching with rigid topology.	Cloud-native, virtualized (SDN/NFV) , elastic routing with dynamic optimization.
3. Cost Structure	High CAPEX/OPEX due to dedicated TDM links, manual routing, and signaling overhead.	Lower, compute/bandwidth-based cost model aligned with modern IP routing.
4. Treatment of Voice Traffic	Designed for high volumes of legacy voice; per-minute cost components.	Optimized for VoLTE/VoIP , media-gateway evolution, and IP-native flows.
5. Treatment of Data / OTT Traffic	Not considered; built before OTT/digital platforms emerged.	Fully integrated with A2P, enterprise workflows, OTT verification calls , API-triggered services.
6. Handling of Enterprise / A2P Calls	Not explicitly recognized; legacy routing assumptions.	Explicitly suitable for digital, fintech, e-commerce, and government helplines .
7. Interconnection Mode	Point-to-point TDM interconnect; manual provisioning.	Multi-operator IP peering , distributed interconnection, cloud exchange points.
8. Routing Efficiency	Static routing, congestion-prone switching networks.	AI-driven traffic management , predictive routing, automated congestion control.

Parameter	Current Transit Charge Framework (2005, TDM-Era)	Proposed Future-Ready Transit Charge Framework (IP-Based, Consumer-Centric)
9. Fraud / Spam Protection	Limited; dependent on SS7 validation and static rules.	Strong AI-based fraud/spam detection , spoofing prevention, anomaly scoring.
10. Transparency	Low transparency; complex reconciliation, varying event logs.	High transparency— standardized IP logs , unified API records, regulator visibility.
11. Billing & Reconciliation	Manual reconciliation; frequent disputes due to mismatched CDR formats.	Automated reconciliation using timestamp-synchronized logs , SIP traces, API events.
12. QoS Monitoring	Legacy KPIs focused on TDM switches; not aligned with IP metrics.	Outcome-based QoS metrics : latency, jitter, packet loss, call completion, fraud blocking.
13. Flexibility for New Services	Rigid; does not support 5G, IoT, or low-latency flows.	Fully flexible for 5G, IoT, URLLC, M2M, cloud-based services .
14. Alignment with Modern Traffic Profiles	Misaligned due to decline in legacy voice and SMS.	Aligned with dominant modern traffic types— A2P, enterprise, OTT, digital services .
15. Scalability	Limited vertical scaling; capacity restricted by TDM hardware.	Horizontal scaling , dynamic capacity expansion in cloud-native platforms.
16. Regulatory Alignment	Based on 2003 IUC assumptions; outdated cost benchmarks.	Updated principles aligned with cost-reflective IP networks , global best practices.
17. Consumer Affordability	Higher costs due to legacy inefficiencies may reflect in service charges.	Lower routing/transit cost → more affordable calls, helplines, verifications .

Parameter	Current Transit Charge Framework (2005, TDM-Era)	Proposed Future-Ready Transit Charge Framework (IP-Based, Consumer-Centric)
18. Consumer Reliability	Higher probability of congestion and call failures on TDM routes.	Better reliability— redundant IP paths, automatic failover, AI-optimized routing.
19. Consumer Transparency	Consumers lack clarity on interconnection failures and hidden costs.	Greater transparency through digital logs, public dashboards, clear service chains.
20. Consumer Protection	Limited protection from spoofed calls, arbitrage-based fraud, and routing abuse.	Strong protection via AI fraud engines, cross-operator analytics, secure signaling.
21. Implementation Complexity	High, due to outdated systems and limited automation.	Lower; automated monitoring, SDN control planes, simplified cost models.
22. Future-Readiness	Does not address digital services, OTT, enterprise calling, or 5G.	Fully future-ready for India's Digital Economy, 5G/IoT ecosystem , and enterprise innovation.
23. Overall Consumer Impact	Higher cost, lower reliability, reduced transparency and weaker protection.	Improved affordability, reliability, transparency, and digital safety.

Q19. The existing interconnection regulatory framework provides for application of origination, carriage, transit, transit carriage and termination charges for various levels of interconnections for PSTN-PSTN, PLMN-PLMN, PLMN PSTN. Based on the interconnection

regulatory framework suggested in your response in Questions 1, 2 and 3 above, should there be a review of these charges? Kindly justify your response.

Comments :

1. This response is submitted from a **consumer-centric and public-interest perspective**, highlighting how a comprehensive review of interconnection charges—covering **origination, carriage, transit, transit carriage, and termination**—is essential in India’s evolving digital ecosystem. As networks migrate from **legacy TDM** to **IP-based interconnection**, and as 5G, IoT, enterprise messaging, and OTT services reshape traffic flows, a modern approach to interconnection charges is required to safeguard **affordability, reliability, transparency, and protection from hidden costs** for consumers.

2. Why a Review of Interconnection Charges is Necessary

2.1 Technological Advancements

a) IP-Based Interconnection

- Modern networks increasingly rely on **VoIP, VoLTE, ViLTE, RCS**, and **SIP-based** signalling.
- IP-based interconnects reduce the need for multiple charging layers such as transit carriage and enable **direct, low-latency connections**.
- The cost structure in IP networks is different—driven by **capacity**, not by distance or circuit occupation.

b) Cloud-Native Routing & SDN/NFV

- Operators now deploy **cloud-native core networks**, enabling dynamic routing and AI-based optimization.
- These technologies reduce operational cost and eliminate physical transit dependencies, making **legacy transit charges outdated**.

c) AI-Driven Traffic Engineering

- Machine learning tools predict congestion and shape traffic efficiently.
- Costs increasingly relate to **compute, spectrum, and orchestration**, not circuit-switching.

d) Growth of 5G, IoT & Enterprise Traffic

- 5G will generate massive **M2M/IoT signalling and micro-bursty traffic** that traditional per-minute/ per-SMS charging cannot model.
- Modern interconnection systems prefer **capacity-based or usage-neutral frameworks**.

2.2 Industry Changes Necessitating Review

a) Migration Away from TDM

- The number of TDM-based POIs is rapidly shrinking.
- Maintaining parallel legacy systems for a few traffic streams escalates avoidable cost.

b) Decline of Traditional Voice/SMS

- OTT voice and messaging significantly reduce P2P voice/SMS volumes.
- Enterprise A2P messaging and digital services dominate traffic patterns, demanding transparent, cost-based interconnect regimes.

c) Emergence of New Business Models

- Hosted voice, CPaaS, RCS Business Messaging, conversational AI platforms, and hybrid OTT-telco models disrupt traditional revenue flows.
- Without rationalised interconnection charges, these innovations may face barriers or create **distorted retail pricing**, ultimately harming consumers.

3. Why Consumers Need a Revised Interconnection Charge Framework

a) Affordability

Consumers directly or indirectly bear interconnection costs. Modern technology has reduced actual operational cost; however, **legacy charges inflate retail tariffs**.

b) Reliability

A modern charging regime encourages:

- deployment of **redundant IP POIs**,
- end-to-end quality measurement,
- lower failure rates.

c) Transparency & Elimination of Hidden Costs

A cost-based and simplified framework prevents:

- opaque transit carriage fees,
- unnecessary multi-operator routing,
- disputes that lead to service disruptions or degraded QoS.

d) Consumer Protection & Trust

A futuristic charging system reduces:

- call drops from overloaded or under-provisioned POIs,
- SMS delays affecting banking/OTP services,
- price distortions between on-net/off-net behavior.

4. Proposed Methodology for Reviewing and Implementing a Modern Framework

4.1 Cost-Based Charging Principles

TRAI may adopt:

- **Long-Run Incremental Cost (LRIC)** for origination, carriage, and termination
- **Marginal Cost–Zero** model for IP transit (where incremental routing cost \approx zero)
- Capacity-based pricing where applicable (Gbps/month instead of per minute)

This approach prevents over-recovery and encourages fair investment.

4.2 Outcome-Linked QoS Metrics

Interconnection charges should be tied to measurable outcomes:

- **Call Setup Success Rate (CSSR)**
- **Post-Dial Delay (PDD)**
- **Average Completion Ratio**
- **SMS/OTP Delivery Time**, especially for enterprise traffic
- **Interconnection Congestion < 0.5%** consistently

Operators failing QoS thresholds may face:

- disincentives,
- penalties,
- reduction in charge ceilings.

4.3 Regulator Dashboards

TRAI may introduce **public-facing dashboards** showing:

- real-time POI congestion,
- QoS for interconnection traffic,
- disputes and resolution timelines,
- on-net vs off-net performance.

This enhances **transparency, trust**, and encourages compliance.

4.4 Phased Rollout

A practical and balanced approach may follow three phases:

Phase 1: Harmonization (0–12 months)

- Rationalize origination, transit, and termination charges under an interim cost-based regime.
- Zero-rate TDM transit where alternative IP POIs exist.

Phase 2: IP-Centric Charging (12–24 months)

- Mandate IP-based interconnect for new POIs.
- Transition high-volume routes to all-IP.
- Introduce capacity-based or hybrid charging.

Phase 3: All-IP Framework (24–36 months)

- Sunset circuit-based transit charging.
- Implement uniform, simplified interconnection regime across PSTN–PSTN, PLMN–PLMN, and PLMN–PSTN.
- Enforce AI-driven monitoring and auto-scaling as a requirement.

4.5 Multilingual Consumer Communication

Operators should be required to inform consumers about:

- how interconnection reforms benefit them,
- why on-net/off-net price differences are disappearing,
- improved QoS expectations.

Communication must be:

- in **regional languages**,
- through SMS, IVR, websites, and mobile apps.

This strengthens consumer empowerment and digital inclusion.

5. Conclusion: Alignment with Global Best Practices & Consumer Protection

A review of interconnection charges is essential to align India's framework with global best practices:

- **Europe:** Zero termination rates for many services; IP interconnect is the norm.
- **USA:** Bill-and-keep models dominate; transit charges minimal.
- **Asia-Pacific:** Rapid migration to capacity-based charging for VoIP and 5G core.

Reforming India's interconnection charges will:

- eliminate outdated cost elements,
- encourage investment in all-IP networks,
- reduce retail tariffs and hidden charges,
- improve reliability of essential services (voice, SMS, digital transactions),
- strengthen consumer trust in telecom networks,
- support innovation and next-generation services.

In summary, a revised, modern, consumer-centric interconnection regime is not only justified but urgently needed. It will ensure affordability, reliability, transparency, and digital empowerment for India's 1.4 billion consumers.

Comparison Table: Current vs Proposed Interconnection Charge Framework

Aspect	Current Framework	Proposed Future-Ready Framework
1. Technology Basis	Primarily TDM-based interconnection; IP deployed unevenly; legacy POIs continue.	All-IP, SIP-based interconnection with cloud-native routing, SDN/NFV, and AI-driven traffic engineering.
2. Charging Principles	Per-minute / per-message charging based on circuit occupation; distance-based elements still embedded indirectly.	Cost-based and capacity-oriented (Gbps/month), marginal-cost model for IP transit, LRIC-based origination/termination.
3. Origination Charges	Separate and not always cost-reflective; based on legacy switching costs.	Simplified LRIC-based origination aligned to IP cost structures; encourages efficient routing.
4. Termination Charges	Vary across networks; tied to legacy costs; may create on-net/off-net price differentials.	Move toward harmonized or near-zero termination , reducing arbitrage and eliminating retail distortions.
5. Transit / Transit Carriage Charges	Several layers of charges (transit, carriage, tandem) depending on routing across LSAs and tandem switches.	Sunset legacy transit layers ; in IP routing, incremental cost \approx zero; capacity-based cross-connect may replace multi-layer tariffs.
6. Carriage Charges (NLDO/ILDO)	Per-minute carriage; impacts long-distance call costs; legacy TDM backhaul.	Capacity-based carriage for long-distance IP routing, neutral to service type (voice, video, IoT signalling).
7. Traffic Patterns	Dominated by P2P voice and SMS; predictable, circuit-based flows.	Enterprise A2P, OTT voice, IoT signalling , and 5G micro-bursts dominate; requires flexible, real-time monetisation.

Aspect	Current Framework	Proposed Future-Ready Framework
8. OTT and Cloud Services	Not fully integrated into interconnection cost structures; creates traffic imbalance perceptions.	Unified, technology-neutral interconnection model supporting OTT integration, hosted voice, CPaaS, RCS, conversational AI.
9. Quality of Service (QoS)	QoS obligations not tightly linked to interconnection charges; limited visibility into POI congestion.	Outcome-linked QoS metrics (CSSR, PDD, SMS latency), auto-scaling IP POIs, and TRAI dashboards for transparency.
10. Dispute Environment	Frequent disputes over capacity, timing of augmentation, billing of multilayer transit; risk of service degradation.	AI-monitored POIs , transparent dashboards, auto-triggered capacity augmentation, minimal billing disputes.
11. Consumer Impact	Consumers exposed to hidden costs due to opaque transit practices; on-net/off-net price differences persist.	Lower tariffs, uniform pricing, faster OTPs, fewer call drops , faster dispute resolution, and stronger digital trust.
12. Interoperability & Flexibility	Multiple POI types; inconsistent formats; high overhead for maintaining parallel TDM+IP networks.	Fully interoperable IP POIs , standardized SIP profiles, cloud-native orchestration, and reduced operational overhead.
13. Regulatory Burden	Heavy compliance load for legacy metrics, physical POI management, and circuit provisioning.	Simplified, digital-by-default regulation with real-time reporting, API-based compliance, and automated QoS analytics.

Aspect	Current Framework	Proposed Future-Ready Framework
14. Rollout Approach	No unified timeline for TDM sunset; fragmented IP transition.	Phased migration (0–36 months): interim harmonization → IP-centric charging → all-IP interconnection.
15. Consumer Communication	Limited and mostly operator-led; consumers unaware of interconnect-driven QoS issues.	Mandatory multilingual consumer communication on price benefits, improved QoS, and IP transition roadmap.

Justification for the Proposed Framework

The proposed future-ready framework is justified because India’s telecom networks have already shifted from legacy TDM architectures to IP-based, cloud-native systems where the true incremental cost of routing is drastically lower and no longer correlated with circuit occupation or distance. Modern technologies—VoLTE, VoIP, 5G core, SDN/NFV, AI-driven routing, and massive IoT signalling—require an interconnection regime that is capacity-based, transparent, and aligned with global benchmarks. Legacy multi-layer transit and carriage charges artificially inflate consumer tariffs, create on-net/off-net disparities, and trigger disputes that risk service disruptions. A harmonized, cost-based IP interconnection model eliminates these distortions while improving reliability, reducing hidden costs, and strengthening consumer trust. By linking charges to measurable QoS outcomes, ensuring real-time transparency through regulator dashboards, and adopting a phased migration path, TRAI can ensure that the interconnection framework continues to protect consumers, promotes

investment, supports new digital services, and keeps India aligned with global best practices for next-generation communications.

Q20. For termination of emergency calls/SMSs from one TSP's network to another TSP's network, should there be a provision of any additional charges other than applicable IUC? If so, what should be the charges and the basis thereof?

Comments :

1. This response is submitted from a **consumer-centric and public-interest perspective**, emphasizing that emergency communications must remain **universally accessible, affordable, reliable, and free of commercial barriers**. As India transitions to next-generation **IP-based emergency networks (NG-112)**, it is critical to ensure that the interconnection framework for emergency calls/SMSs does not introduce any additional cost to consumers—directly or indirectly.

2. Should Additional Charges Be Prescribed Beyond IUC? – Consumer-Centric Position : **No.**

No. Additional charges for termination of emergency calls/SMSs should *not* be prescribed.

Emergency communications are a public good and form the backbone of **national safety, disaster management, health services, women/child helplines, and digital public infrastructure**.

Any extra charge—even if indirectly applied—risks:

- reduced access for low-income users,
- inconsistent call handling across networks,
- potential refusal or downgrading of emergency traffic,
- slower migration to IP-based NG-112 systems.

A modern regulatory approach must treat emergency communication as a **consumer right, not a commercial transaction.**

3. How Technology Advancements Strengthen the Case Against Additional Charges

3.1 IP-Based Emergency Routing (NG-112 / NG-911 Models)

Modern emergency networks route calls through:

- **IP Multimedia Subsystems (IMS),**
- **SIP-based signaling,**
- **cloud-based Emergency Communication Platforms.**

In such environments, incremental routing cost is extremely low—often close to *zero*, eliminating the economic rationale for additional termination charges.

3.2 AI-Driven Prioritization & Contextual Routing

AI engines now enable:

- dynamic call prioritization,
- real-time congestion management,
- intelligent routing to nearest PSAP (Public Safety Answering Point),
- automated location tagging.

These technologies operate efficiently only when emergency traffic is **free from billing friction**.

3.3 Migration to VoLTE / VoWiFi / 5G Voice

As PSTN networks sunset:

- emergency calls increasingly originate from packet-switched domains,
- termination relies on **IP-to-IP interconnect**, not circuit occupancy.

Legacy cost models no longer apply.

3.4 5G / IoT Emergency Ecosystem

Emergency communications now include:

- IoT fire alarms,
- vehicle crash detection (eCall),
- wearable health monitors,
- telematics distress signals.

These operate at micro-bursty, low-cost signalling patterns incompatible with any per-call surcharge model.

3.5 Convergence with OTT Platforms

Across the world, emergency calling is integrated with:

- smartphone SOS features,
- vehicle safety systems,
- health apps.

Charging TSP-level termination fees would complicate integration and diminish consumer safety.

4. Industry Changes Supporting a Zero/No Additional Charge Regime

a) Decline of Circuit-Switched Emergency Traffic

Most emergency calls now originate from VoIP/VoLTE, rendering legacy termination cost structures irrelevant.

b) Need for Unified India-Wide Emergency Response

India is moving toward:

- a **single national emergency number (112)**,
- unified PSAPs,
- centralized dispatch systems.

Differential operator charges would fragment this ecosystem.

c) Responsibility to Maintain Public Trust

Emergency calls must never be subject to:

- commercial negotiation,
- inter-operator disputes,
- billing reconciliation complexity.

A zero-charge regime ensures *zero risk of disruption*.

5. Consumer Benefits of a Zero/Additive-Free Charging Policy

5.1 Universal and Equal Access

Every citizen—irrespective of:

- income,
- device type,
- home network,
- roaming status—

must have equal access to emergency services.

5.2 Affordability and Digital Inclusion

Free emergency calling is essential for:

- rural communities,
- low-income users,
- children and elderly,
- vulnerable groups (women, victims of violence).

5.3 Reliability During Crises

Eliminating commercial layers ensures:

- faster routing,
- lower post-dial delay,
- higher call completion ratios,
- reduced risk of congestion at POIs.

5.4 Protection from Hidden Costs

Consumers must never pay or subsidize emergency termination costs, even passively through:

- increased tariffs,
- special packs,
- off-net/on-net differentials.

5.5 National Security and Disaster Preparedness

During floods, fires, pandemics, earthquakes, and cyber emergencies, the network must be:

- free of billing barriers,
- optimized for prioritization,
- inherently resilient.

6. Proposed Methodology for Implementation

6.1 Zero or Strictly Marginal-Cost Charging

TRAI may mandate:

- **Zero termination charge** for emergency calls/SMSs, OR
- **Marginal cost–zero model** (cost-based but capped at zero).

This is aligned with global NG-112 and NG-911 best practices.

6.2 Outcome-Linked QoS Metrics

Operators should be evaluated on:

- Call setup success rate for emergency calls
- Post-dial delay
- Time to route to PSAP
- SMS delivery time (for distress messages)

- Network availability during crises

Non-compliance may trigger corrective actions or penalties.

6.3 Regulator Dashboards

TRAI may develop a public dashboard showing:

- emergency call QoS,
- PSAP accessibility,
- operator performance,
- congestion events.

This increases transparency and builds public trust.

6.4 Phased Rollout Framework

Phase 1 (0–12 months):

- Freeze all emergency-related charges at zero.
- Standardize SIP/IMS routing profiles.

Phase 2 (12–24 months):

- Introduce NG-112 compatible interconnect architecture.
- Implement AI-based prioritization systems.

Phase 3 (24–36 months):

- Full migration to cloud-native NG-112 nationwide.
- Automated monitoring and enforcement.

6.5 Multilingual Consumer Communication

Operators must inform citizens—through SMS, IVR, apps, and outreach—that:

- emergency calls are free,
- accessible from any network,
- reliable even without balance or active recharge.

This is crucial for public safety and inclusion.

7. Conclusion: Global Best Practices & Consumer Protection

International benchmarks overwhelmingly support **no additional charges** for emergency communications:

- **USA – NG-911:** Zero termination charge; cost absorbed as public safety obligation.
- **EU – eCall / NG-112:** All emergency communication is free and prioritized.
- **Asia-Pacific:** Universal no-charge emergency calling integrated with 4G/5G networks.

Adopting the same approach in India ensures:

- universal access during crises,
- no risk of commercial discrimination,
- faster emergency response,
- seamless integration with NG-112,
- protection of low-income and vulnerable consumers,
- alignment with next-generation IP technologies.

In summary: additional charges for termination of emergency calls/SMSs should NOT be prescribed. A zero-charge, IP-ready, consumer-centric regime best serves national safety, digital inclusion, and public trust.

Comparison Table: Current vs Proposed Emergency Charging Framework

Aspect	Current Framework	Proposed Future-Ready Framework (NG-112/Next-Gen)
1. Charging Principle	No explicit unified policy; emergency calls are generally free for consumers, but inter-TSP termination may involve applicable IUC principles.	Zero termination charge or marginal-cost-zero model for all emergency calls/SMSs; no additional charges beyond IUC.
2. Technology Basis	Predominantly legacy PSTN/TDM routing , with partial IP/VoLTE integration.	Fully IP-based emergency routing , SIP/IMS signaling, cloud-native PSAPs, NG-112 architecture.
3. Emergency Call Routing	Routed through mixed TDM + IP paths; dependent on traditional POIs; variable PDD and latency.	AI-driven, context-aware routing directly to nearest PSAP; lower latency and guaranteed prioritization.
4. Interconnection Method	Hybrid: SS7/TDM for older networks, SIP for newer; inconsistent processing.	Unified all-IP interconnection for emergency traffic across all TSPs with common SIP profiles.

Aspect	Current Framework	Proposed Future-Ready Framework (NG-112/Next-Gen)
5. Cost Characteristics	Circuit-based cost perception persists; operators maintain parallel legacy systems.	IP routing has near-zero incremental cost , removing rationale for extra charges.
6. Support for 4G/5G Emergency Services	Limited support for advanced emergency features; VoLTE emergency calling not uniformly implemented.	Native support for VoLTE, VoWiFi, 5G voice , IoT distress signals, eCall (vehicle crash alerts), telematics.
7. Reliability and Congestion Handling	Congestion at POIs can delay or block emergency calls during crises; limited real-time visibility.	Automated prioritization, dynamic scaling, and cloud orchestration ensure near-zero congestion risk.
8. Emergency SMS Delivery	SMS routing may face delays or congestion; not optimized for OTP-based distress systems.	Guaranteed low-latency delivery , with measurable QoS targets for emergency SMS.
9. QoS Enforcement	QoS monitoring not specifically tied to emergency interconnection performance; limited transparency.	Outcome-linked QoS metrics: CSSR, PDD, routing time to PSAP, SMS delivery latency; public regulator dashboards.
10. Consumer Protection	Risk of hidden commercial frictions between TSPs; uneven performance across networks.	Uniform national policy ensuring universal, free, non-discriminatory access from any network/technology.
11. Roaming Scenarios	Emergency calls sometimes rerouted with intermediate charges depending on domestic roaming agreements.	All emergency calls (including roaming) treated as zero-charge, highest-priority traffic .
12. Dispute Environment	Inter-TSP disputes on IUC applicability, routing, or	Zero-charge environment eliminates disputes , ensures

Aspect	Current Framework	Proposed Future-Ready Framework (NG-112/Next-Gen)
	capacity augmentation may affect emergency traffic.	uninterrupted emergency service availability.
13. Support for IoT-Based Emergencies	Very limited; not designed for vehicle crash alerts, fire sensors, wearables, etc.	5G-IoT and telematics ready: accepts automated distress signals from sensors and smart devices.
14. Public Awareness & Communication	Mostly operator-led and limited; consumers unaware of emergency calling rules.	Mandatory multilingual communication informing consumers of free access and improvements under NG-112.
15. Alignment with Global Practices	Fragmented and legacy-driven; lacks consistent NG-112/NG-911 structure.	Fully aligned with global best practices: USA (NG-911), EU (NG-112), APAC next-gen models.

Justification for the Proposed Framework

The proposed framework is justified because emergency communications are a core public safety function, not a commercial service, and must remain universally accessible, affordable, and free from inter-operator financial barriers. As India transitions to next-generation IP-based emergency systems—NG-112, VoLTE/VoWiFi emergency calling, 5G- and IoT-driven distress signalling, and AI-enabled routing—the incremental cost of terminating emergency traffic is negligible, rendering any additional charges unnecessary and counterproductive. A zero-charge, outcome-linked, IP-native regime eliminates the risk of inter-operator disputes,

ensures uniform reliability during crises, improves call/SMS prioritization, and enhances transparency through real-time QoS dashboards. Aligning with global best practices (NG-911, NG-112, EU eCall) strengthens public trust, guarantees uninterrupted access for vulnerable populations, and ensures that India's emergency communication architecture remains future-ready and consumer-protective.

Q21. Should the International Termination Charges (ITC) for international incoming calls to India be revised? If yes, what are the considerations necessitating such a revision. Kindly provide your response with justification.

Comments :

1. This response is submitted from a **consumer-centric and public-interest perspective**, recognizing that International Termination Charges (ITC) play a decisive role in determining the affordability, security, and reliability of international voice communications for millions of Indians. With rapid technological shifts, global migration to IP-based interconnection, and rising threats such as spam, spoofing, and international fraudulent calls, a review of the existing ITC regime is both timely and essential.

2. Technology Advancements Supporting a Review of ITC

2.1 IP-Based Interconnection & SIP/IMS Migration

Global telecom ecosystems have moved rapidly toward:

- **IP-based international interconnection,**
- **SIP/IMS-driven voice routing,** and
- **VoIP/VoLTE/VoWiFi** termination at the destination end.

These technologies significantly reduce the real cost of delivering international calls to Indian networks.

2.2 Cloud-Native Interconnects & SBCs

Modern ILDOs and TSPs increasingly use:

- **Cloud Session Border Controllers (SBCs),**
- **Virtualized Media Gateways,**
- **Dynamic load balancing and path optimization.**

The marginal cost per call is falling, enabling more flexible and consumer-friendly ITC frameworks.

2.3 Carrier-Grade Anti-Fraud & Analytics Platforms

With rising international spam and scam calls, operators now deploy:

- **AI-based anomaly detection,**
- **real-time traffic scoring,**
- **honeypot calling patterns,**
- **international signalling analytics.**

These advances make it possible to **tie ITC adjustments to security outcomes**, ensuring protection of Indian consumers.

2.4 STIR/SHAKEN-Like Call Authentication

Global markets are introducing:

- **caller ID authentication frameworks,**
- **cryptographic call signing,**
- **fraud-resistant routing policies.**

A modern ITC regime must encourage adoption of such technologies by making charges **incentive-aligned with security and trustworthiness.**

3. Industry Changes Necessitating an ITC Review

3.1 Shift from TDM to SIP/IMS

Legacy TDM circuits have almost disappeared from international voice ecosystems.

Maintaining older infrastructure for a small subset of traffic is inefficient and creates inflated cost assumptions for ITC.

3.2 OTT Substitution

International calling volumes have declined due to:

- WhatsApp,
- FaceTime,
- Telegram,
- Google Meet, etc.

Thus, ITC should reflect:

- **reduced cost recovery needs,**
- the need to **promote legitimate channels,**
- and **prevent grey-route arbitrage.**

3.3 Changing ILDO Business Models

ILDOS increasingly operate:

- cloud-based routing hubs,
- hybrid OTT–carrier partnerships,
- pay-as-you-go IP interconnection.

A revised ITC structure should align with these models rather than rely on outdated circuit-based cost logic.

3.4 Grey-Route and Spoofing Pressures

High ITC in any jurisdiction tends to:

- incentivize bypass routes,
- encourage SIM-box fraud,
- increase caller ID spoofing risks.

A **balanced, rational ITC** reduces grey traffic, protects consumer trust, and enhances lawful interception.

4. Key Consumer Benefits from Revising ITC

4.1 Affordability and Accessibility

Rational ITC ensures:

- cheaper international calls,
- wider family & diaspora connectivity,
- inclusion for migrant workers and low-income households.

4.2 Enhanced Reliability

IP-native routing with optimized least-cost paths improves:

- call setup success,
- post-dial delay,
- call completion ratios.

4.3 Anti-Fraud and Anti-Spam Protection

A modern ITC framework can be tied to:

- authenticated caller ID,
- verified ILDO partners,
- secure routing channels.

This protects consumers against:

- spoofed “international bank calls”,
- fraudster UPS/loan/credit scams,
- fake job or immigration calls.

4.4 Greater Transparency

Consumer experience improves when:

- grey routes are eliminated,
- routing is secure and visible,
- pricing is aligned to actual costs.

Transparency leads to stronger digital trust in India’s telecom grid.

5. Proposed Methodology for Implementation

5.1 Cost-Based and Outcome-Linked Pricing

TRAI may adopt a hybrid model:

- **Cost-based ITC** reflecting modern IP cost structures,
- **Outcome-linked incentives** tied to:
 - authenticated calls (STIR/SHAKEN-like),
 - compliance with anti-spoofing policies,
 - lower spam/fraud metrics.

5.2 Differentiated Classes for Voice Types

Charges may vary by:

- **International PSTN-originated voice,**
- **IP-originated authenticated voice,**
- **OTT partner voice (carrier-integrated),**
- **Enterprise/verified call originators.**

This discourages risky unverified routes and rewards trusted, authenticated traffic.

5.3 Strict QoS and Security SLAs

Operators should adhere to measurable SLAs:

- Call Setup Success Rate (CSSR)
- Post Dial Delay (PDD)
- Answer-Seizure Ratio (ASR)
- Call completion reliability
- Caller ID authentication rate
- Spam/fraud detection thresholds

Non-compliant routes may face:

- penalties,
- increased ITC (disincentive),
- or blocking via regulatory direction.

5.4 Phased Rollout

Phase 1 (0–12 months):

- Freeze ITC while conducting revised cost studies reflecting IP migration.
- Introduce pilot authentication frameworks (STIR/SHAKEN-like).

Phase 2 (12–24 months):

- Implement differentiated ITC tiers based on authentication, security, and QoS.
- Mandate IP-only international interconnect for large routes.

Phase 3 (24–36 months):

- Move to a fully IP-native, security-first, fraud-resistant ITC model.
- Real-time automated monitoring, secure routing, and global interoperability.

5.5 Regulator Dashboards

TRAI may launch real-time dashboards showing:

- ITC-based routing trends,
- origin-country spoofing statistics,

- grey-route attempts detected,
- ILDO compliance,
- overall international QoS.

This increases transparency and strengthens consumer trust.

5.6 Multilingual Consumer Communication

TSPs should inform users—via SMS, IVR, websites, and apps—about:

- reduction in spam international calls,
- better caller ID protection,
- enhanced reliability,
- affordability improvements.

This ensures public awareness and reinforces digital trust.

6. Conclusion: Prioritizing Consumer Protection & Global Best Practices

A revision of India's ITC regime is not only justified but necessary in the context of:

- **global IP migration,**
- **declining cost structures,**
- **growing fraud threats,**
- **OTT-driven substitution,** and
- **next-generation international interconnect standards.**

A modern, balanced ITC:

- improves affordability for Indians living abroad and their families in India,

- strengthens anti-fraud and anti-spam protection,
- reduces grey routes and illegal bypass,
- encourages authenticated, secure global connectivity,
- ensures transparency and accountability,
- and aligns India with international best practices (USA, EU, Singapore, UAE).

In summary, revising ITC using a consumer-centric, IP-driven, security-first approach will protect consumers, enhance digital trust, and build a future-ready international voice ecosystem for India.

Comparison Table: Current vs Proposed ITC Framework

Aspect	Current ITC Framework	Proposed Future-Ready ITC Framework
1. Technology Basis	Primarily legacy TDM/SS7 international interconnect; partial SIP/IMS adoption.	All-IP, SIP/IMS-native international interconnect , cloud SBCs, virtual gateways, STIR/SHAKEN-ready architecture.
2. Cost Structure	Based on outdated circuit-switching costs; assumes fixed per-minute cost recovery.	IP cost model with near-zero incremental cost , capacity-based and usage-agnostic pricing.
3. Charge Philosophy	Flat ITC with minimal differentiation; focused on revenue recovery for TSPs/ILDOs.	Cost-based + outcome-linked ITC , incentivizing security, authentication, and QoS compliance.
4. Routing Framework	Mix of TDM and IP routing; inconsistent quality and latency; limited monitoring.	Cloud-native routing , AI-optimized paths, secure SIP

Aspect	Current ITC Framework	Proposed Future-Ready ITC Framework
		trunks, real-time anomaly detection.
5. Caller ID & Authentication	Limited authentication; prone to spoofing and grey-route manipulation.	STIR/SHAKEN-like authentication , verified caller ID, mandatory anti-spoofing checks.
6. Fraud & Grey-Route Exposure	Higher ITC encourages grey-route bypass, SIM boxes, spoofed CLI.	Rationalized ITC reduces bypass incentives , ensures traceability, and improves lawful interception.
7. Treatment of OTT/VoIP Traffic	Ambiguous; often bypasses proper ILDO routing due to high cost and no proper integration.	Integrated OTT-carrier ecosystem , lower barriers for legitimate IP-originated international calls.
8. QoS Management	Minimal linkage between ITC and service quality; variable CSSR, PDD, ASR.	Strict QoS SLAs tied to ITC tiers: CSSR, PDD, ASR, jitter, packet loss, call completion.
9. Security Requirements	Reactive fraud monitoring; post-facto analysis; minimal accountability.	AI-driven proactive anti-fraud analytics , honeypots, international signalling surveillance.
10. Consumer Impact	Higher cost of international calls; vulnerability to spoofed spam/fraud calls; inconsistent quality.	Lower cost, higher reliability , reduced spam/fraud , authenticated calling, transparent pricing.
11. ILDO Economic Model	Volume-dependent revenue, tied to legacy settlements.	Cloud-native, flexible ILDO model , incentivizing secure and authenticated traffic.

Aspect	Current ITC Framework	Proposed Future-Ready ITC Framework
12. International Roaming & Global Integration	Legacy roaming interconnect arrangements; variable termination pathways.	Unified IP-based global interconnect , harmonized routing and authentication standards.
13. Regulatory Oversight	Limited real-time visibility; reliance on operator reporting.	Regulator dashboards with real-time traffic quality, spoofing patterns, and route compliance.
14. Pricing Flexibility	One-size-fits-all ITC irrespective of origin country, authentication status, or voice type.	Differentiated ITC classes: verified traffic, PSTN-originated, OTT-integrated, enterprise authenticated.
15. Consumer Awareness	Minimal communication on international call safety or spam protection.	Mandatory multilingual consumer communication on fraud reduction, authentication benefits, and tariff transparency.
16. Alignment with Global Practice	Lagging behind US, EU, Singapore, UAE IP-based international frameworks.	Fully aligned with global next-gen interconnect standards and anti-fraud norms (STIR/SHAKEN, NGN IPX).

Justification for the Proposed Future-Ready ITC Framework

The proposed ITC framework is justified because international voice traffic today is predominantly IP-based, authenticated, and cloud-routed, making legacy per-minute, circuit-switched cost assumptions obsolete. Modern technologies such as SIP/IMS interconnect, cloud SBCs, AI-driven fraud analytics, and STIR/SHAKEN-like caller authentication drastically reduce

the marginal cost of terminating international calls while simultaneously enabling stronger protection against spoofing, grey routes, and scam calls targeting Indian consumers. A revised, rationalized, outcome-linked ITC structure incentivizes secure, authenticated, high-quality traffic and discourages fraud-prone bypass routes. This directly benefits consumers through lower international calling costs, higher reliability, improved caller ID integrity, and reduced exposure to financial fraud. Aligning India's ITC framework with global best practices ensures a future-ready, secure, and transparent international voice ecosystem that prioritizes consumer protection above revenue-driven legacy models.

Q22. Is there a need to address the issue of telemarketing and robo-calls within the interconnection framework? If yes, kindly provide your inputs on the possible approaches. Kindly justify your response. A.6. The Telecommunication Interconnection (Reference Interconnect Offer) Regulations, 2002

Comments :

Unsolicited telemarketing and robocalls continue to be the single largest source of consumer irritation, financial fraud, and erosion of trust in the telecom ecosystem. While TRAI has rightly introduced regulatory controls under TCCCPR-2018, the *actual transport* of such calls happens through interconnection points between TSPs—making the **interconnection framework** an essential control layer.

Therefore, **telemarketing and robocalls *must* be addressed within the interconnection framework**, leveraging modern technologies, global best

practices, and authenticated traffic pathways to ensure consumer protection.

1) Technology Advancement Enabling Interconnect-Level Control

Modern telecom architectures now allow robust, intelligent, and real-time interventions at the interconnection layer:

a) Caller Authentication (Digital Signatures / Verification Tokens)

- Using cryptographic signing of caller identity (similar to STIR/SHAKEN) during interconnect handover.
- Ensures only authenticated enterprise and telemarketer calls are allowed to enter the network.

b) Analytics-Based Spam Scoring

- Real-time scoring engines at the interconnect can evaluate calling patterns, behaviour anomalies, and crowd-sourced reputation.
- Calls marked with high spam scores are automatically *throttled*, *challenged*, or *blocked*.

c) Real-Time Blocking at the Interconnect

- Cloud-native SBCs allow call rejection before the traffic enters the terminating network, reducing consumer exposure.

d) Cloud-Native SBCs and SDN/NFV

- Scalable, programmable interconnects capable of enforcing dynamic spam policies.

- Allow per-category treatment of calls (verified enterprise, marketing, grey-route risky calls, robocalls, etc.).

e) AI-Based Anomaly Detection

- Detects mass-calling bots, sudden spikes, rotating CLI patterns, and cross-border spoofing.
- Enables automated containment of malicious campaigns within seconds.

Conclusion:

Technological maturity now makes it possible—and necessary—to embed spam and telemarketing controls directly into the interconnection layer.

2) Industry Changes Necessitating Interconnect-Level Controls

a) Rapid Growth of A2P / Enterprise Messaging and Calling

Consumers increasingly receive OTPs, banking alerts, e-commerce updates, and service notifications. Without strong interconnect controls:

- fraudulent OTP-bypass calls rise,
- cost to consumers and enterprises increases,
- legitimate A2P channels suffer dilution.

b) Grey-Route Abuse

Unscrupulous entities bypass registered telemarketer channels by:

- spoofing CLIs,
- using international routes for domestic marketing,
- blending robocalls with OTT signalling.

Only interconnect-level inspection can reliably detect grey route patterns.

c) OTT Blending and Hybrid Call Paths

Enterprises use SIP aggregators and cloud contact centres. These must be authenticated during interconnect hand-in, or else spam will exploit unverified OTT pathways.

d) Cross-Border Spam and Fraud

Fraudsters use:

- overseas VoIP,
 - SIM farms,
 - compromised PBXs
- to insert malicious calls into India.

Interconnect-level authentication and traffic marking are required to protect consumers.

e) Rise of Verified Enterprise Calling

Enterprises are adopting:

- branded caller ID,
- verified business profiles,
- reputation scores.

To ensure trust, the interconnection regime must differentiate between:

- **verified calling traffic**, and
- **unknown / unverified traffic**.

3) International Practice Supporting Interconnect-Level Measures

a) STIR/SHAKEN Attestation – USA & Canada

- Mandatory authentication of caller identity at interconnect.
- Classifies calls as A/B/C based on verification level.
- Has significantly reduced spoofing.

b) Do-Not-Call Enforcement – USA, UK, Australia

- Interconnection traffic is monitored to ensure that registered entities do not violate DNC norms.
- Penalties applied at the interconnect level for rule-breaking callers.

c) Traceback Protocols – US FCC / Industry Traceback Group

- Enables identification of the first ingress point of spam/robocalls.
- Prevents blame-shifting between operators.

d) EU / Ofcom Measures Against Robocalls

- CLI authentication during interconnect.
- Mandatory blocking of invalid, unallocated, or spoofed numbers at interconnection.
- International gateway validation.

Conclusion:

Global regulators treat robocalls as an *interconnection challenge* and enforce controls at the carrier handover point. India should adopt similar forward-looking mechanisms.

4) Consumer Benefits From Addressing Telemarketing Within Interconnection

a) Greater Safety and Fraud Prevention

Blocking spoofed and fraudulent calls before they reach consumers protects:

- elderly users,
- rural users,
- financial novices.

b) Enhanced Trust in Telecom Networks

Consumers can rely on:

- verified caller display,
- authenticated enterprise calling,
- consistent spam reduction.

c) Improved Affordability

Reducing spam reduces:

- network load,
- operator compliance cost,
- consumer's indirect cost of fraudulent transactions.

d) Higher Reliability

Legitimate traffic (bank OTPs, emergency calls) faces less congestion because spam is filtered pre-network.

5) Proposed Methodology for Implementation

A phased, standards-based approach aligned with TCCCPR, TIR-2018, and future Telecommunications Act rules:

A) Interconnect-Level Requirements (RFO / RIO Additions)

1. Caller Authentication

- Every interconnect call must carry a signed identity header.
- Verified telemarketers receive *high attestation*.
- Unknown or suspicious sources get *low or no attestation*.

2. Spam and Anomaly Controls

TSPs must deploy:

- AI-based anomaly detection engines,
- spam scoring,
- pattern analytics,
- grey-route detection.

3. Invalid and Suspicious CLI Blocking

Mandatory blocking of:

- unallocated numbers,
- short CLI,
- known spoofing patterns.

B) Tiered Treatment of Traffic

Traffic Category	Treatment
Verified Enterprises	Priority routing, high attestation, consumer trust indicators
Registered Telemarketers	Controlled throughput, continuous monitoring
Unknown Traffic	Lower trust; subject to throttling, additional screening
Suspicious/Grey-route Traffic	Automated blocking at the interconnect
Robocalls/Malicious Traffic	Mandatory rejection with traceback initiation

C) QoS & Security SLAs

Include performance and safety obligations in interconnection agreements:

- < 2s spam decision latency
- Mandatory traceback within 24 hours
- Call signature verification success rate
- Identity header integrity measurements
- Fraud incident reporting timelines

D) Regulatory Dashboards

Regulators and TSPs should maintain:

- real-time dashboards on spam volumes,
- traceback results,

- attestation levels by TSP,
- action taken on violators.

E) Phased Rollout

Phase 1:

- Caller authentication pilot (3–6 months).
- Interconnect SBC upgrades.

Phase 2:

- Mandatory attestation for domestic enterprise calls.
- Blocking of invalid + high-risk CLIs.

Phase 3:

- International inbound authentication.
- Real-time traceback federation across TSPs.

Phase 4:

- Full integration with consumer apps, DND registry, and fraud analytics ecosystem.

F) Multilingual Consumer Communication

To ensure inclusivity:

- push notifications explaining authenticated calls,
- regional language awareness campaigns,
- bank/enterprise communication on verified calling.

Conclusion: Clear Justification

Integrating telemarketing and robocall controls into the interconnection framework is **essential** for India's consumer protection, network hygiene, and global credibility.

International experience shows that **interconnect-level caller authentication, attestation, and real-time anomaly detection** are the only scalable methods to combat spoofing, grey routes, and robocall fraud.

A strengthened interconnection regime will deliver:

- safer communication,
- trustworthy enterprise calling,
- reduction in harassment and fraud,
- analytics-driven governance aligned with global best practices.

Therefore, telemarketing and robocalls *should definitively be addressed within the interconnection framework*, with a structured, technology-enabled, consumer-centric, and phased implementation plan as outlined above.

Q23. Is there a need to revise 'The Telecommunication Interconnection (Reference Interconnect Offer) Regulation, 2002'? If yes, kindly provide the specific revisions. Kindly provide your response with justification.

Comments :

The RIO-2002 framework was designed for a circuit-switched, TDM-dominated era. Today's telecom environment has transformed with IP/SIP-IMS interconnection, cloud-native routing, AI-driven operations, 5G

architecture, and global security threats. To ensure consumer protection, reliability, affordability, and trust, **RIO-2002 requires a comprehensive, forward-looking revision.**

1) Technology Advancement Supporting Revision

a) IP/SIP-IMS Interconnection

The ecosystem has fundamentally moved from:

- TDM → IP
- E1/T1 → SIP trunks
- SS7 → SIP/DIAMETER/HTTP-based signalling

Current interconnection agreements must reflect:

- SIP profiles,
- codecs,
- media encryption,
- header integrity rules,
- QoS requirements for VoLTE/VoWiFi/5G calls.

b) Cloud-Native POIs and SDN/NFV

Operators now use:

- virtual SBCs,
- cloud interconnect fabrics,
- dynamic routing,
- programmable interconnect policies.

RIO-2002 does not cover cloud-native POI discovery, automated scaling, or security hardening.

c) Programmable SBCs & Rich Policy Controls

Modern interconnect SBCs can enforce:

- caller ID authentication,
- traffic shaping,
- anomaly detection,
- encrypted media,
- API-driven provisioning.

These capabilities require updated RIO clauses on:

- protocol behaviour,
- authentication,
- fraud controls,
- analytics visibility.

d) AI/Analytics for Interconnect Management

AI now drives:

- real-time QoS management,
- spam detection,
- fraud control,
- congestion prediction.

RIO-2002 does not mandate sharing of analytics, dashboards, or predictive indicators across TSPs.

e) 5G Network Slicing & Rich Communications

Slicing introduces differentiated classes of services.

Interconnect agreements must reflect:

- priority routing for emergency calls,
- RCS/IMS profiles,
- QoS tiers for voice/video/data,
- latency-sensitive services.

f) Authentication & Identity Assurance

With increasing fraud, verification of:

- caller identity,
- enterprise signatures,
- network attestation levels

is crucial.

RIO-2002 does not address identity management at interconnection.

2) Industry Changes Necessitating Revision

a) Migration from TDM to All-IP

Over 90% of global voice networks have migrated.

Legacy RIO-2002 obligations do not match:

- SIP-IMS interop,
- HD voice interoperability,
- VoLTE interconnect,
- VoWiFi/handover rules.

b) Rise of OTT, CPaaS, and A2P / Enterprise Traffic

Enterprise calling (banking OTP, customer care, e-commerce) drives most call volume.

Current RIO-2002 cannot address:

- OTT-originated SIP traffic,
- CPaaS aggregators,
- grey-route misuse,
- enterprise authentication requirements.

c) Cross-Border Ingress & Global Routing

International VoIP ingress requires:

- identity verification,
- anti-spoofing,
- monitoring of suspicious patterns,
- international signalling integrity.

RIO-2002 predates this threat landscape.

d) IoT, VoWiFi, VoLTE & Hybrid Access Technologies

Modern devices generate calls via:

- Wi-Fi calling,
- satellite relay,
- IoT modules,
- fixed-mobile convergence.

Interconnect obligations must define:

- authentication,
- routing,
- QoS,
- fallback procedures.

e) Security & Fraud Pressures

The rise of:

- robocalls,
- spoofing,
- SIM-farms,
- SMS termination fraud,
- bank-fraud calls

demands an interconnect-layer security framework absent in RIO-2002.

3) International Practice Supports Updating the RIO

a) ETSI/3GPP SIP-IMS Interconnect Profiles

EU operators use standardized:

- SIP header rules,
- codec negotiations,
- emergency call marking,
- QoS parameters.

India's RIO-2002 lacks these.

b) STIR/SHAKEN Attestation – USA/Canada

Mandatory authentication of caller identity at interconnect prevents:

- CLI spoofing,
- robocall fraud,
- cross-border scams.

c) Ofcom/EU Transparency, QoS & Security Rules

International regulators mandate:

- KPIs for voice quality,
- interoperability standards,
- transparency on traffic categories,
- regular reporting of fraud/scam calls.

d) NG-112 / NG-911 Emergency Handling Frameworks

Emergency frameworks require:

- priority routing,
- IP-based location sharing,
- redundancy,
- high-availability interconnects.

RIO-2002 lacks provisions for next-gen emergency requirements.

Conclusion:

India's RIO must align with global next-gen interconnect frameworks to ensure fair competition and consumer protection.

4) Consumer Benefits From Revising RIO-2002

a) Affordability

- Efficient IP interconnect reduces cost of voice termination.
- Better fraud control reduces indirect financial burden on consumers.

b) Reliability

- Cloud-native redundancy lowers call drops.
- SLA-driven QoS assures better voice/video quality.
- High-availability IP interconnection ensures continuity during disasters.

c) Trust & Transparency

- Verified caller identity reduces fear of scam calls.
- Better policing of grey routes protects consumers from fraud.

d) Protection from Spam, Spoofing & Robocalls

- Interconnect-level screening stops harmful calls *before* they reach consumers.
- Authentication-based routing boosts consumer confidence.

5) Proposed Methodology for Revising the RIO

Below is a forward-looking implementation plan:

A) Update RIO-2002 with Specific Clauses on Technology

1. IP-Based Interconnection

Mandatory SIP-IMS profiles covering:

- codecs,
- header integrity,

- encryption (TLS/SRTP),
- authentication,
- SIP OPTIONS heartbeat.

2. Cloud-Native POI Requirements

- auto-scaling capability,
- virtual POIs,
- geo-redundancy rules,
- disaster recovery obligations.

3. Programmable SBC Requirements

Mandate SBC features:

- caller authentication,
- fraud detection,
- real-time analytics exposure,
- protocol validation.

B) QoS & Security SLAs

Include measurable obligations:

- call setup success rate,
- PDD,
- jitter/latency thresholds (especially for VoLTE/5G),
- spam detection success,
- TRACEBACK adherence timelines.

C) Standardized APIs

Introduce APIs for:

- interconnect provisioning,
- traffic classification,
- signature/attestation validation,
- analytics insights (per hour, per region, per TSP),
- fraud alert exchange.

D) Dashboards for Transparency

Mandate shared dashboards for:

- real-time interconnect utilization,
- QoS performance,
- fraud/spam events,
- call attestation levels,
- outage notifications.

E) Phased Rollout

Phase 1: Foundation (0–6 months)

- SIP-IMS mandatory for all new interconnections.
- New RIO template issued by TRAI.
- Basic security headers required.

Phase 2: Security (6–12 months)

- Caller authentication (Indian STIR/SHAKEN).
- Blocking of invalid/unused CLIs.
- Shared fraud intelligence exchange.

Phase 3: Analytics & Quality (12–24 months)

- Mandatory QoS dashboards.
- Predictive congestion analytics.
- Cloud-native POI rollout.

Phase 4: Consumer Transparency (24–36 months)

- Verified caller identity indicators for consumers.
- multilingual consumer education campaigns.
- ongoing compliance audits.

F) Multilingual Consumer Communication

To ensure inclusivity across India:

- periodic SMS advisories,
- posters in retail outlets,
- consumer-facing dashboards,
- awareness messages in regional languages about verified calling.

Conclusion: Clear Justification

Revising the **RIO-2002** is essential to safeguard consumer interest, ensure fair competition, and maintain India's leadership in next-generation telecom services. The current framework was created for a TDM world; it cannot support today's **IP-based, cloud-native, fraud-prone, enterprise-driven, and 5G-enabled ecosystem**.

A modernized RIO will:

- strengthen **consumer protection** against fraud and spam,

- enhance **affordability**,
- guarantee **reliability** and service quality,
- enable **fair competition** among operators, and
- align India with **international best practices** such as STIR/SHAKEN, ETSI SIP-IMS profiles, and next-gen emergency frameworks.

Therefore, RIO-2002 should be comprehensively revised with an IP-centric, secure-by-design, analytics-enabled, and consumer-protective architecture, ensuring a transparent, trustworthy, and globally competitive telecom ecosystem.

Q24. For the purpose of interconnection, is there a need to revise the current categories of ‘Services’ and ‘Activities’ to determine Significant Market Power (SMP)? Kindly provide your response with justification.

Comments :

India’s telecom landscape has shifted dramatically from legacy voice/SMS-centric interconnection to an **IP-driven, cloud-based, OTT-integrated, enterprise-heavy ecosystem**. The categories of "services" and "activities" used to determine Significant Market Power (SMP) were created for a very different era. To protect consumers and ensure fair, competitive, and resilient networks, these categories now need **comprehensive revision**.

1) Technology Advancements Support Updating SMP Categories

a) IP-Based Interconnection

Modern networks rely on:

- SIP/IMS interconnects
- encrypted signaling
- cloud-native SBCs
- programmable routing

Legacy SMP categories built around TDM voice/SMS no longer capture:

- IP voice quality control
- packet-based prioritization
- authentication-based routing
- interconnect analytics

b) OTT Platforms and Next-Generation Services

OTT communication services influence:

- call volumes,
- consumer behaviour,
- international traffic,
- enterprise calling substitution.

Ignoring OTT-communication influence leads to improper SMP assessment.

c) Cloud-Native POIs

Interconnection is no longer physical.

Operators use:

- virtual POIs,
- cross-connect fabrics,

- cloud-exchange hubs.

These cloudified activities are central to market power—but are not addressed in old SMP categories.

d) AI-Driven Traffic Analytics

Operators deploy AI for:

- congestion prediction,
- anomaly detection,
- routing optimization,
- robocall/spoofing checks.

The ability to control analytics-driven routing influences market power and should be recognized as an SMP activity.

e) 5G, Network Slicing, IoT Services

5G transforms interconnection from:

- fixed QoS → dynamic SLA-driven services
- monolithic networks → slice-based services
- simple voice/SMS → mission-critical IoT, low-latency services

Thus, SMP assessment must include:

- slice-level interconnect control,
- edge-routing capabilities,
- IoT traffic aggregation.

2) Industry Changes Necessitate Revising SMP Categories

a) Migration from Legacy Voice/SMS to Data-Driven Services

Consumers rely more on:

- VoLTE/VoWiFi
- OTT audio/video calling
- CPaaS/A2P services
- push notifications

Legacy SMP categories centered around call minutes and SMS volumes no longer represent market influence.

b) Rise of A2P/Enterprise Messaging and Calling

Enterprises use:

- cloud CPaaS platforms
- SIP aggregators
- enterprise verified calling

Control over enterprise channels is a significant competitive advantage. Old SMP definitions do not include this.

c) OTT Substitution and Hybrid Models

Consumers seamlessly shift between:

- network voice,
- OTT voice/video,
- RCS,
- Wi-Fi calling.

Ignoring OTT substitution gives an incomplete picture of market dominance.

d) Cross-Border Traffic & Grey Routes

Operators with major international interconnect roles influence:

- anti-fraud controls
- international QoS
- cross-border pricing

This role must be treated as an SMP-relevant activity.

e) Decline of Circuit-Switched Interconnect

SMP categories based on:

- TDM capacity,
 - E1-based traffic,
 - SS7 signaling
- are obsolete.

3) International Practice Strongly Supports Updating SMP Framework

a) EU SMP Framework (European Commission & BEREC)

EU regulators use:

- market-specific SMP analysis,
- evolving service scopes (not static voice/SMS),
- next-generation access obligations.

They revise categories regularly based on technological and behavioral shifts.

b) Ofcom Market Review (UK)

Ofcom includes:

- OTT influence,
 - cloud interconnect roles,
 - traffic routing control,
 - data-driven service categories
- when assessing SMP.

c) FCC Competitive Safeguards (USA)

FCC categorizes:

- VoIP interconnection,
 - enterprise access services,
 - IP-based routing functions
- as part of SMP evaluation.

d) ITU Guidelines

ITU encourages:

- dynamic market definition,
- periodic revision of categories,
- alignment with technological evolution,
- consumer protection safeguards.

India must stay aligned with these global benchmarks.

4) Consumer Benefits From Revising SMP Categories

a) Affordability

Proper SMP identification prevents:

- excessive termination charges,
- discriminatory pricing,
- cost-padding in enterprise channels.

Consumers ultimately benefit from lower service costs.

b) Reliability

By capturing modern interconnect functions, regulators can ensure:

- no anti-competitive routing decisions,
- no artificial congestion by dominant players,
- better QoS for VoLTE/5G services.

c) Transparency

Updated SMP categories will:

- expose dominant behavior in cloud-based services,
- ensure fair access for smaller TSPs and CPaaS players,
- create clarity for consumers about service guarantees.

d) Protection From Anti-Competitive Behaviour

New SMP categories help prevent:

- discriminatory throttling,

- blocking of OTT traffic,
- unfair interconnect negotiation leverage,
- manipulation of enterprise channels.

This directly protects consumer interest.

5) Proposed Methodology for Implementing the Revised SMP Framework

A) Updated Categories of Services and Activities

New categories should include:

1. IP Voice & IMS Interconnection Services

- SIP signaling
- IMS-based QoS
- voice/video codecs
- VoLTE/VoWiFi

2. OTT-Influenced Communication Services

- OTT offload/hand-in
- hybrid RCS services
- aggregator-based calls

3. A2P/Enterprise/CPaaS Services

- enterprise call origination
- verified calling
- cloud contact centre interconnect

4. Cloud-Native and Virtual Interconnection Activities

- virtual POIs
- programmable routing
- interconnect via cloud exchanges

5. AI-Powered Interconnect Analytics Activities

- traffic shaping
- anti-spam controls
- congestion prediction
- real-time fraud detection

6. 5G/IoT Interconnection Services

- slice-based interconnect
- low-latency SLA routing
- IoT gateway interconnect

B) Outcome-Based SMP Assessment

Shift from volume-based metrics to outcome-based indicators:

Outcome KPIs

- control over QoS for IP voice,
- ability to influence cloud interconnect routing,
- share of enterprise/A2P handoff capability,
- degree of dependency by smaller networks,
- access leverage in 5G/IoT edge infrastructure,
- impact on consumer experience metrics.

C) Regulator Dashboards

TRAI should maintain dashboards for:

- SIP failure rates,
- VoLTE interconnect QoS,
- enterprise traffic routing fairness,
- anti-spam compliance,
- cross-border traffic transparency,
- congestion incidents.

Dashboards enforce accountability.

D) Phased Rollout Plan

Phase 1: Framework Design (0–6 months)

- publish revised categories;
- industry consultation;
- drafting of updated SMP guidelines.

Phase 2: Data Gathering (6–12 months)

- TSP reporting on IP interconnect, OTT substitution metrics;
- enterprise/A2P traffic mapping.

Phase 3: SMP Assessment & Obligations (12–24 months)

- apply outcome-based analysis;
- impose obligations on SMP entities (transparent interconnect, QoS assurances, non-discrimination).

Phase 4: Consumer Outreach (24–36 months)

- multilingual public communication;
- awareness on rights;
- dashboards online for public visibility.

Conclusion: Clear Justification

Revising the categories of “services” and “activities” used to determine SMP is essential for modern telecom regulation. The existing framework—built on legacy voice/SMS markets—cannot safeguard consumer interest in a world dominated by IP interconnection, OTT calling, cloud-native routing, enterprise communications, and 5G/IoT services.

A modernized SMP framework will:

- prevent anti-competitive behaviour,
- ensure fair and non-discriminatory interconnection,
- promote affordable and reliable services,
- enhance transparency and trust,
- align India with EU/Ofcom/FCC/ITU best practices.

Therefore, TRAI should revise the SMP service/activity categories using a technology-aware, outcome-based, consumer-protective methodology to build a fair, competitive, and future-ready interconnection ecosystem.

Q25. Should the publication of Reference Interconnect Offers (RIOs) on the websites of Telecom Service Providers (TSPs) be mandated? Kindly

justify your response. **A.7. The Telecommunication Interconnection (Charges and Revenue Sharing) Regulations, 2001**

Comments :

1. Introduction: Why Transparency in Interconnection Matters Today

Interconnection is the backbone of India's telecom ecosystem—every voice call, SMS, data session, and enterprise communication ultimately depends on transparent, non-discriminatory interconnection arrangements. As technologies evolve and traffic patterns shift from legacy TDM to IP-based, cloud-native, and OTT-driven models, **lack of publicly accessible Reference Interconnect Offers (RIOs)** increases the risk of **disputes, opaque pricing, and anti-competitive behavior**, which eventually impacts **consumer affordability, service reliability, and trust**.

Mandating the publication of RIOs on TSP websites, therefore, is not only a regulatory requirement but a **consumer-centric necessity** for a modern digital economy.

2. Technology Advancements Enable Seamless, Real-Time Transparency

a) Digital Transparency Portals

Modern web portals allow real-time publication, versioning, and archiving of RIO documents, ensuring all stakeholders—including consumers, enterprises, small ISPs, and regulators—can access updated information without delay.

b) Cloud-Native Interconnect Management Systems

TSPs increasingly use cloud-native interconnect platforms with automated workflows, making it easy to publish standardized RIO documents directly from operational systems. This reduces administrative burden while improving accuracy.

c) AI-Driven Compliance Dashboards

AI tools can automatically track:

- changes made to RIOs,
- interoperability conditions,
- pricing updates,
- version history,

and can also **alert TRAI** if any discrepancy or delay in publication occurs. This makes online publication not only desirable but **effortless and tamper-proof**.

3. Industry Changes Make Publication Even More Critical

a) Transition from TDM to IP-Based Interconnection

As operators migrate to **VoIP, VoLTE, VoWiFi, SIP-IMS**, and cloud interconnection, RIOs increasingly include:

- QoS parameters,
- security norms,
- signaling requirements,
- ENUM, SBC, and packet routing conditions.

Publishing these details publicly prevents ambiguity and ensures fair negotiation between operators of varying sizes.

b) Rise of OTT and Enterprise Traffic

OTT voice/video apps, CPaaS players, and enterprise messaging providers require interconnection clarity. Public RIOs ensure **non-discriminatory access** and prevent preferential treatment.

c) Increasing Number of Interconnection-Related Disputes

Opaque, unpublished RIOs have historically contributed to interconnection disputes. A transparent online repository can drastically reduce:

- billing disagreements
- POI provisioning disputes
- alleged discriminatory practices
- RIO interpretation discrepancies

d) Growing Number of Small and Regional ISPs

Smaller ISPs and rural providers often lack insight into the terms offered by larger operators. Online RIO publication levels the playing field and **promotes competition**, ultimately benefiting consumers.

4. International Best Practices Strongly Support RIO Publication

a) European Union (EU)

Under the EU SMP framework, operators with market power must **publish RIOs online** with:

- technical conditions,
- pricing tables,
- SLAs,

- non-discrimination clauses.

b) Ofcom (UK)

Ofcom mandates transparency in interconnection agreements and RIO publication to ensure **fair access and prevent margin squeeze**.

c) Federal Communications Commission (FCC – USA)

FCC rules require clear, publicly available interconnection and access terms, particularly in IP-based environments.

d) ITU Guidelines

ITU-T recommendations emphasize transparent disclosure of interconnect terms to:

- reduce disputes,
- enhance market efficiency,
- promote consumer interest.

Thus, mandating RIO publication on TSP websites aligns India with **global regulatory best practices**.

5. Consumer Benefits: Transparency Strengthens Consumer Welfare

a) Affordability

Transparent interconnection terms reduce disputes and hidden costs, lowering the overall cost structure of telecom services—which ultimately translates into **lower tariffs for consumers**.

b) Reliability

Clear interconnection conditions help avoid service disruptions due to technical or commercial disagreements, ensuring:

- stable call connectivity,
- seamless roaming,
- dependable emergency services.

c) Transparency and Digital Trust

Consumers gain confidence when they know that interconnection terms are open and non-discriminatory. This strengthens **digital trust** in the telecom ecosystem.

d) Protection from Anti-Competitive Practices

Publicly accessible RIOs prevent:

- arbitrary pricing,
 - discriminatory treatment,
 - hidden interconnection barriers,
- thereby safeguarding consumer rights.

6. Proposed Methodology for Implementation

A) Mandatory Online Publication of All RIOs

TRAI may mandate that every TSP must publish:

- complete RIO (pricing, technical, operational, and SLA terms),
- version history and date of last update,
- applicable addendums and amendments,
- interconnection categories (voice/SMS/IP/enterprise).

These documents should be in **searchable and downloadable formats (PDF, HTML)**.

B) Regulator-Monitored Transparency Dashboards

A TRAI-hosted dashboard may:

- aggregate RIO links from all TSPs,
- show version changes and compliance status,
- issue alerts if RIO updates are delayed or incomplete.

C) Standardized RIO Templates

TRAI can prescribe a uniform structure covering:

1. General terms
2. Technical specifications
3. Financial/charge details
4. QoS parameters
5. Security norms
6. SLAs and KPIs
7. Dispute resolution mechanism

A standardized template eliminates ambiguity and ensures fair competition.

D) Phased Rollout

1. Phase 1 (0–3 months):

- Publish existing approved RIOs online.
- Provide links to TRAI.

2. Phase 2 (3–6 months):

- Implement compliance dashboards.
- Update RIOs in standardized format.

3. Phase 3 (6–12 months):

- Integrate AI-driven monitoring and automated version tracking.
- Begin multilingual public communication.

E) Multilingual Consumer Communication

TSPs may be required to:

- publish summaries in **English + Indian languages**,
 - explain interconnection transparency in consumer-friendly terms,
 - include FAQs and public awareness material,
- to ensure informed consumer participation.

7. Conclusion: A Necessary Step Aligned with Global Best Practices

Mandating the publication of RIOs on TSP websites is an **essential reform** for a modern, competitive, and consumer-centric telecom ecosystem. Given the rapid transition to IP-based networks, rise of OTT and enterprise communication models, and increasing complexity of interconnection arrangements, **online RIO transparency strengthens fairness, reduces disputes, promotes efficiency, and enhances digital trust.**

This measure mirrors best practices adopted by the EU, Ofcom, FCC, and ITU, and ensures that India's telecom market remains **open, competitive, and aligned with global standards.**

Above all, it ensures that **consumers benefit from affordable, reliable,**

and transparent telecom services, which is fundamental to Digital India and the broader public-interest mandate of TRAI.

Comparison Table: Current vs Proposed RIO Transparency Framework

Aspect	Current Framework (As per Telecommunication Interconnection (Charges & Revenue Sharing) Regulations, 2001)	Proposed Framework (Future-Ready, Consumer-Centric Approach)
Availability of RIOs	RIOs are shared mostly upon request or during bilateral negotiations between operators; no mandatory public disclosure.	Mandatory publication of complete RIOs on each TSP's official website, easily accessible without login.
Transparency Level	Limited transparency; stakeholders often lack visibility into interconnection terms, charges, and technical conditions.	High transparency through publicly accessible, standardized RIO documents, visible to all stakeholders including consumers, small ISPs, and enterprises.
Update Mechanism	Updates often communicated through internal channels; no real-time public record of changes or version history.	Version-controlled online publication with timestamps, change logs, and automated update notifications via TRAI dashboard.
Format & Structure	RIO formats differ across TSPs; lack of uniformity leads to interpretational challenges.	Standardized RIO template prescribed by TRAI covering technical, commercial, QoS, security, and SLA parameters.

Aspect	Current Framework (As per Telecommunication Interconnection (Charges & Revenue Sharing) Regulations, 2001)	Proposed Framework (Future-Ready, Consumer-Centric Approach)
Regulatory Monitoring	Monitoring is manual, complaint-based, and often triggered after disputes.	AI-driven and dashboard-based monitoring by TRAI for compliance, timely updates, and automated alerts for discrepancies.
Accessibility for New/Small Operators	Smaller ISPs and start-ups face information asymmetry; negotiation power is low without transparent RIOs.	Equal access through published RIOs, promoting fair competition and enabling new entrants to interconnect efficiently.
Dispute Resolution	Higher probability of disputes due to lack of clarity and inconsistent RIO communication.	Reduced disputes as all terms are openly available, minimizing ambiguity and ensuring uniform understanding.
Technical Modernization	Framework still reflects legacy TDM conditions; limited reference to IP-based interconnection (VoLTE, SIP-IMS, VoWiFi).	RIOs must clearly define IP-based interconnection , cloud-native routing, SBC configurations, security norms, and QoS metrics.
Consumer Awareness	Consumers have no access to interconnection terms; transparency is indirect and limited.	Multilingual public summaries explaining interconnection transparency and consumer benefits, enhancing digital trust.
International Alignment	Partially aligned; lacks mandatory publication	Fully aligned with EU SMP framework, FCC transparency rules, Ofcom publication

Aspect	Current Framework (As per Telecommunication Interconnection (Charges & Revenue Sharing) Regulations, 2001)	Proposed Framework (Future-Ready, Consumer-Centric Approach)
	requirements followed in EU, USA, UK.	mandates, and ITU-T guidelines.
Implementation Method	Static, document-driven, and compliance is reactive.	Dynamic, phased rollout with cloud-based publication, standardized templates, and regulator-linked dashboards.
Consumer Impact	Opaque interconnection costs may indirectly affect consumer tariffs and service reliability.	Transparent interconnection promotes affordability, reliability, fair competition, and anti-competitive safeguards for consumers.

The proposed RIO Transparency Framework is essential to modernize India’s interconnection ecosystem, align domestic practices with global standards, and ensure that consumers benefit from affordable, reliable, and transparent telecom services. The current framework, developed under the 2001 Regulations, was appropriate for a voice-centric, TDM-based era. However, the telecom landscape has fundamentally transformed due to the shift toward IP-based interconnection, cloud-native networks, and the exponential rise of OTT and enterprise communication. The absence of mandatory public publication of RIOs has resulted in persistent information asymmetry, limited competition, and recurring interconnection disputes. A future-ready transparency framework is therefore both timely and necessary.

Under the existing arrangements, RIOs are typically exchanged only upon request between operators, resulting in restricted visibility and inconsistent formats across TSPs. This limits the ability of new entrants, small ISPs, and regional operators to negotiate equitable interconnection terms. The lack of uniformity contributes to operational ambiguity and hinders efficient network integration, which indirectly affects consumers through delayed interconnections, potential service disruptions, and higher costs passed on through tariffs.

The proposed framework introduces **mandatory online publication** of all RIOs on TSP websites, supported by standardized templates prescribed by TRAI. This ensures universal accessibility, greater interpretability, and non-discriminatory access to technical and commercial information. Additionally, integrating **AI-driven compliance dashboards** and automated update mechanisms enables proactive monitoring, ensuring that any changes are published promptly with full version control and transparency. This transition from a reactive to a proactive monitoring structure will significantly reduce disputes related to charges, POI provisioning, and technical specifications.

Global regulatory best practices overwhelmingly support RIO publication. The EU's SMP-based transparency obligations, Ofcom's mandatory online disclosure rules, the FCC's interconnection transparency mandates, and ITU-T recommendations on interconnect openness all demonstrate the importance of public RIOs in promoting fair competition and safeguarding consumer rights. Aligning with these frameworks positions India as a leader in transparent interconnection policy, particularly critical in the context of 5G, IoT, cloud interconnects, and enterprise communication growth.

For consumers, the benefits are substantial. Transparent interconnection costs foster competitive pricing, leading to more affordable tariffs. Clear technical parameters enhance service reliability, reduce call failures, and minimize disruptions. Public oversight of RIOs builds digital trust and strengthens the consumer protection mandate by preventing anti-competitive behaviour such as discriminatory pricing or restricted access.

In summary, the proposed RIO Transparency Framework is a necessary evolution that supports a modern, competitive, and consumer-centric telecom ecosystem. It reduces disputes, promotes fair competition, strengthens regulatory oversight, aligns with global standards, and ensures that the Indian consumer is the ultimate beneficiary. This reform directly contributes to the objectives of Digital India, universal service, and long-term network resilience.

Q26. Should there be any interconnection charges? If yes, kindly provide details about the following: a. the types of infrastructure charges to be levied, 138 b. the guiding principles for determining such charges along with ceiling, if required, and c. determination of time-based escalation methodology, if required. Kindly provide your response with justification.

Comments :

A response on interconnection charges can easily slide into dry economics, yet the stakes are delightfully human. Every voice call, every OTP, every network hand-shake between operators ultimately determines how affordable, reliable, and trustworthy digital communication feels to the Indian consumer. A modern framework for interconnection charges can't

cling to its TDM-era ancestry; it must acknowledge a world in which packets sprint across 5G cores, cloud-native POIs auto-scale on demand, and artificial intelligence manages traffic flows that no human could track second-to-second. Below is a forward-looking, consumer-oriented response that draws these threads together.

Consumer-Centric Response: Should Interconnection Charges Be Levied?

1. The Core Question: Why Charges Exist at All

Interconnection charges have always existed to compensate one network for using another's resources. In the past, this meant switching equipment, SS7 signaling, copper trunks, and TDM-based POIs. But telecom today is less about metal and more about software. When networks become cloud-native and elastic rather than fixed and rigid, the way we think about interconnection costs must also evolve.

The question is not simply "Should we levy charges?" but "What form should those charges take in a modern, IP-based, consumer-first ecosystem?" That framing keeps the focus on efficiency, fairness, and consumer benefit.

2. Technology Shifts Demand a New Interconnection Philosophy

A) IP-Based Interconnection

With VoLTE, VoWiFi, IMS, SIP, and packet-based routing, interconnection no longer depends on heavy physical E1 lines. The dominant costs today relate to:

- SBC capacity

- routing intelligence
- IP domain security
- QoS management
- virtualized network functions

This shifts the economics from **per-minute or per-SMS consumption** toward **infrastructure provisioning and quality assurance**.

B) Cloud-Native POIs

POIs now scale like cloud applications—automatically, elastically. The cost is not the port, but:

- compute cycles
- virtual resource scaling
- storage for logs
- cyber-security and signaling verification systems

Charging models should therefore reflect **capacity and performance**, not legacy circuit-style units.

C) AI-Driven Traffic Management

AI already orchestrates routing, congestion management, and anomaly detection for fraud (grey routes), DDoS, and spoofed signaling. These systems require:

- continuous data ingestion
- trained models
- processing power

These technology layers are not “optional luxuries”; they are essential operational safeguards. A well-calibrated interconnection fee can support their reliability without inviting overcharging.

D) 5G SA, Network Slicing & IoT

5G introduces differentiated requirements:

- ultra-low latency slices
- high-reliability slices
- massive IoT slices

These create differentiated **cost structures**. A one-size-fits-all interconnection charge would be scientifically inaccurate. A modern framework must allow granularity without complexity.

3. Industry Changes Reinforce the Need for Clarity

A) Migration from Legacy TDM → All-IP

Operators are sunsetting TDM. Maintaining parallel legacy platforms is expensive and unnecessary. Interconnection charges should no longer be based on TDM-era assumptions.

B) Rise of OTT, CPaaS & Enterprise Messaging

OTT substitution complicates settlement ecosystems. Meanwhile, enterprise messaging and A2P traffic still rely on operator networks for authentication, security, and delivery quality. Transparent charges discourage:

- hidden markups

- discriminatory pricing
- grey-route exploitation

C) New Business Models

- CPaaS aggregators
- global cloud telephony players
- IoT connectivity providers

introduce multi-party flows. Interconnection charges must be simple, predictable, and scalable.

D) Grey-Route & Fraud Pressures

Fraud thrives where pricing is opaque. Cost-based, transparent interconnect charges reduce arbitrage opportunities and protect consumers from suspicious call routing patterns.

4. International Practices Strongly Support Cost-Based, Transparent Interconnect Pricing

European Union

The EU uses **pure cost-based models** for termination. Rates approach zero for many services, while still maintaining transparency and non-discrimination.

FCC (USA)

FCC mandates:

- transparency in interconnection
- reasonableness in charges

- safeguards against market abuse

Ofcom (UK)

Ofcom imposes strong protections when a TSP holds Significant Market Power (SMP). Charges must:

- reflect efficient cost
- avoid margin squeeze
- be publicly documented

ITU Guidelines

ITU-T emphasizes:

- transparency
- fairness
- cost-orientation
- technology neutrality

India's framework should mirror these principles while remaining sensitive to domestic realities.

5. Consumer Benefits: Why This Matters To the Public

Affordability

Cost-based interconnection keeps tariffs stable. Excessive or arbitrary charges eventually flow into consumer bills.

Reliability

Transparent, predictable interconnection improves:

- call completion
- QoS
- routing efficiency
- emergency service performance

Transparency

Clear public charges discourage disputes and unknown markups. Transparency always works in the consumer's favour.

Protection from Anti-Competitive Behavior

A uniform, standardized, regulator-monitored framework prevents:

- discriminatory access
- price barriers
- unfair advantages for dominant players

A vibrant, competitive market ultimately means better prices and performance for consumers.

6. Proposed Methodology for Implementation

A) Types of Interconnection Charges (Modernized Taxonomy)

A future-ready structure may include:

- 1. Infrastructure Provisioning Charge**
 - covers SBC, routing, monitoring, and cyber-security layers.
- 2. Capacity-Based Charge**
 - Mbps/Gbps/virtual port capacity, not per-minute.

3. **QoS/SLA Compliance Charge**

- optional charge tied to measurable KPIs (latency, jitter, packet loss).

4. **Minimal Termination Charge**

- if required, aligned to international norms approaching zero.

B) Guiding Principles

- **Cost-based** and not revenue-maximizing
- **Technology neutral**
- **Non-discriminatory** across operators
- **Simple and predictable**
- **Transparent to all stakeholders**

C) Ceilings & Floors

TRAI may define:

- maximum allowable charges based on efficient cost
- minimum thresholds (if needed) to avoid predatory pricing

D) Time-Based Escalation Methodology

Charges may:

- decline over time as networks become more efficient
- phase out legacy elements
- adjust automatically based on audited cost data

This creates predictability for TSPs and protection for consumers.

E) Regulator Dashboards

A TRAI-hosted dashboard can track:

- published interconnection charges
- historical versions
- cost justification submissions
- compliance status

AI-driven alerts can flag deviations instantly.

F) Phased Rollout

1. **Phase 1:** publish current charges with clear documentation.
2. **Phase 2:** shift to capacity-based, IP-centric units.
3. **Phase 3:** integrate dashboards, automated compliance, and cloud-native provisioning.
4. **Phase 4:** multilingual public-facing awareness to enhance transparency.

G) Multilingual Consumer Communication

Public explanations in major Indian languages ensure consumers understand:

- how interconnection affects tariffs
- how transparency prevents overcharging
- how digital trust is strengthened

7. Conclusion: Why a Modernized Interconnection Charge Framework Is Necessary

A modern framework for interconnection charges is essential for maintaining fairness, transparency, and efficiency in India’s rapidly evolving telecom landscape. Technology has changed, traffic flows have changed, business models have changed—and the regulatory philosophy must evolve with equal agility.

A **cost-based, transparent, technologically neutral, and consumer-first structure** protects India from anti-competitive practices, supports the growth of 5G and IoT ecosystems, and shields consumers from hidden costs and service instability. By drawing from global best practices while respecting domestic realities, India can ensure that interconnection remains:

- fair,
- efficient,
- innovation-friendly, and
- strongly aligned with consumer protection.

This approach strengthens India’s digital infrastructure, supports Digital Bharat, and ensures that every consumer enjoys affordable, reliable, and trustworthy communication services.

Comparison Table: Current vs Proposed Interconnection Charging Framework

Aspect	Current Framework	Proposed Future-Ready, Consumer-Centric Framework
Nature of Interconnection Charges	Primarily based on legacy TDM interconnection concepts; voice-centric; limited differentiation across IP, cloud, or enterprise interfaces.	Modernized, technology-neutral charges reflecting IP-based interconnect, cloud-native POIs, SBC gateways, edge nodes, and 5G/IoT slicing infrastructure.
Cost Basis	Historically determined charges with limited granularity; based on TDM cost models.	Strict cost-based + outcome-linked charging aligned with EU/ITU principles; ceilings to prevent over-recovery and anti-competitive practices.
Transparency of Charges	Limited visibility; charges often disclosed only during bilateral negotiations; no real-time publication.	Mandatory public disclosure of all interconnection charges on TSP websites + TRAI dashboards with version history and AI-driven monitoring.
Treatment of IP-Based Interconnection	Partially defined; no uniform structure for SIP-IMS, VoLTE/VoWiFi, cloud POIs, or virtual interconnects.	Detailed, dedicated IP charging framework covering SIP trunks, virtual POIs, cloud nodes, edge data centers, session control, and security layers.
OTT / Enterprise / CPaaS Traffic Models	No clear distinction between traditional voice and enterprise/OTT traffic; leads to disputes.	Clear classification of P2P, A2P, OTT voice, enterprise CPaaS, IoT/5G slices, with differentiated cost models and QoS-linked conditions.

Aspect	Current Framework	Proposed Future-Ready, Consumer-Centric Framework
Grey Route Mitigation	Limited economic deterrence; inconsistent charges create arbitrage.	Uniform, transparent, IP-aligned charges closing arbitrage gaps, integrated with AI-driven fraud analytics and real-time route validation.
QoS & SLA Linkages	Weak linkage between charges and QoS; parameters mostly voice-centric.	Outcome-based charging where charges reflect SLA commitments (latency, jitter, packet loss, 5G slice isolation, emergency services reliability).
Regulatory Monitoring	Manual, reactive monitoring; disputes often arise post-facto.	AI-driven monitoring , dashboards, and automated alerts for anomalies, delays, and discriminatory behavior.
Dispute Frequency	Higher—due to ambiguity and lack of transparency in cost models and charge applicability.	Lower—due to standardized templates , cost ceilings, public disclosure, and automated compliance systems.
International Alignment	Partially aligned; does not fully reflect EU’s cost-orientation, Ofcom’s SMP duties, FCC transparency rules, or ITU interconnect guidelines.	Fully aligned with global best practices , including EU REC/2014 model, Ofcom’s non-discrimination safeguards, FCC transparency, ITU-T Recommendation D-series.
Flexibility for Innovation	Limited—framework constrains virtual interconnects, cloud nodes,	High—supports innovation such as cloud POIs, programmable interconnects, network slicing, AI-

Aspect	Current Framework	Proposed Future-Ready, Consumer-Centric Framework
	and new enterprise/IoT models.	based routing, and CPaaS ecosystems.
Consumer Impact	Indirect; opaque charges may translate into higher tariffs or degraded QoS.	Direct consumer benefit: affordability, reliability, digital trust, better quality of calls/data, and protection from anti-competitive pricing.
Implementation Style	Static, document-based, inertia in updating charges.	Dynamic, phased rollout with periodic reviews, inflation-indexed ceilings, 3–5 year validity windows, multilingual consumer communication.

Justification for the Proposed Interconnection Charge Framework

The proposed Interconnection Charge Framework is essential to modernize the cost, efficiency, and transparency principles governing India’s interconnection regime. The existing framework was designed for a predominantly TDM-based era, where interconnection was physically intensive, capacity-limited, and cost-heavy. However, India’s telecom ecosystem has transformed: networks now run on IP, cloud-native cores, virtualized POIs, and software-defined routing, while consumers increasingly rely on data, OTT, enterprise messaging, and 5G/IoT services. Continuing with a legacy charging model that does not reflect these structural changes leads to inefficiencies, disputes, and hidden costs that ultimately burden consumers.

Under the current system, interconnection charges are often reactive, operator-specific, and based on legacy cost elements tied to physical circuits, TDM switching, or capacity blocks. This model is increasingly misaligned with cloud-native, scalable, software-defined IP interconnection, where marginal cost per session is significantly lower, but security, QoS, signaling integrity, fraud mitigation, and redundancy require predictable investment. The lack of a modernized cost structure also contributes to grey-route exploitation, inconsistent A2P enterprise pricing, and disputes over POI provisioning—all of which impact consumer experience, either through degraded call quality, delayed service rollout, or increased downstream tariffs.

The proposed framework introduces a balanced, forward-looking structure that preserves affordability while ensuring cost recovery for new-age interconnection infrastructure. It includes transparent, standardized categories of charges—such as IP-POI setup, security and signaling assurance, cloud routing, and QoS slicing—supported by regulator-defined ceilings and cost review cycles. This ensures that charges reflect real-world technological needs without creating room for arbitrary or anti-competitive pricing. The introduction of regulator dashboards, automated reporting, and AI-driven dispute detection further enhances transparency and reduces compliance burden.

Global best practices strongly support such modernization. The EU mandates cost-based, non-discriminatory interconnect principles; Ofcom's SMP safeguards ensure fair pricing and prevent margin squeeze; the FCC emphasizes clarity and transparency; and ITU guidelines endorse IP-agnostic, predictable models aligned with next-generation networks.

Adopting similar principles ensures India remains globally competitive and technologically resilient, particularly as 5G standalone cores, IoT slicing, satellite backhaul, and security standards evolve rapidly.

Most importantly, the proposed reforms significantly benefit consumers. Affordability is protected through ceilings and transparency-driven competition. Reliability improves through investments in redundant, secure, cloud-native POIs. Transparency reduces hidden costs and prevents passing unjustified charges to consumers. Anti-competitive safeguards ensure new entrants, rural ISPs, start-ups, and enterprise providers can interconnect on equal terms—strengthening market diversity and service availability. By shifting to a future-ready, cost-reflective, and regulator-supervised model, India guarantees that interconnection supports Digital India, consumer rights, and long-term network sustainability.

In conclusion, the proposed framework is not just a technical improvement—it is a consumer-centric modernization essential for India's transition to IP-based, cloud-native, and 5G-era communications. It aligns with global best practices, reduces disputes, enhances affordability, and ensures that the benefits of digital connectivity are accessible to every citizen.

Q27. Whether following sections of The Telecommunication Interconnection (Charges and Revenue Sharing) Regulations, 2001: a. Section IV which contains 'Revenue Sharing Arrangements' i.e.

interconnection usage charges. b. Schedule I and II which contains rates of interconnection usage charges. still hold relevance, in view of the subsequent issuance of the Regulation 4 under Section IV which specifies rates of 'Interconnection Usage Charges (IUC) under 'The Telecommunication Interconnection Usage Charges Regulations, 2003'. Additionally, is there an alternative way to organize these two regulations to enhance clarity and ease of understanding? Kindly provide your response with justification. A.8. Telecommunication Interconnection (Port Charges) Regulations, 2001 and Its Amendments

Comments :

1. Need to Review Legacy Provisions of the 2001 Framework

Section IV and Schedules I & II of the **Telecommunication Interconnection (Charges and Revenue Sharing) Regulations, 2001** were designed for a voice-centric, circuit-switched, TDM-based ecosystem. With the issuance of the **Interconnection Usage Charges (IUC) Regulations, 2003**, many commercial, technical, and revenue-sharing provisions were superseded, modified, or rendered redundant.

Today's telecom environment—driven by **IP-based interconnection, cloud-native POIs, AI-driven analytics, 5G slicing, enterprise communication, OTT substitution, and grey-route pressures**—requires a **harmonized and consolidated regulatory structure** rather than fragmented legacy frameworks. Consolidating outdated regulations is essential for transparency, ease of compliance, fair competition, and **consumer protection**.

2. Technology Advancements Necessitating Consolidation

a) IP-Based Interconnection (SIP/IMS/VoLTE/VoWiFi)

The 2001 Regulations were designed around **TDM E1 and circuit-switched interconnection**, whereas today:

- voice is carried over **IP packets**,
- signaling uses SIP and Diameter,
- QoS and SLA parameters differ entirely, and
- many IUC elements are no longer applicable.

A unified framework should reflect the **packet-switched, cloud-native** reality.

b) Cloud-Native, Virtualized POIs

Modern networks rely on:

- cloud SBCs,
 - NFV/SDN routing,
 - geo-redundant POIs,
- which fundamentally change interconnection economics and processes.

Legacy schedules cannot capture these requirements.

c) AI-Driven Traffic Analytics

AI systems now monitor:

- fraudulent traffic,
- grey-route manipulation,
- network load balancing,

- predictive QoS.

This requires modern regulatory expectations absent in the 2001 schedules.

d) 5G, IoT, Network Slicing

5G introduces:

- logical slicing,
 - differentiated QoS,
 - ultra-low-latency traffic classes,
- which require a fresh and simplified regulatory code—not disparate legacy documents.

3. Industry Changes Demand a Unified Regulation

a) Shift from TDM to IP

The industry has almost completed migration from E1/TDM to **SIP, IMS, and cloud-native interconnects**, making several provisions in Section IV & Schedules I–II obsolete.

b) Rise of OTT and Enterprise Traffic

OTT substitution and enterprise CPaaS traffic have redefined traffic flows, requiring **modern interconnection parameters** not reflected in the 2001 schedules.

c) New Business Models

- A2P/flash calling
- CPaaS/SaaS-driven routing

- IoT/industrial automation traffic

These models require clearer, consolidated regulation.

d) Grey-Route and Anti-Fraud Pressures

Fragmented regulations make enforcement harder. A unified code enables **precise compliance and stronger anti-fraud enforcement**.

4. International Practices Support Consolidation

a) EU – Consolidation Under the EECC

The European Electronic Communications Code (EECC) consolidates interconnection rules into a single structure for:

- clarity,
- transparency,
- competitive neutrality.

b) Ofcom – Simplified SMP Frameworks

Ofcom regularly **prunes outdated provisions**, merging overlapping obligations for ease of compliance.

c) FCC – Unified Interconnection Rules

The FCC consolidates interconnection obligations under a unified code, eliminating duplicative and obsolete sections.

d) ITU – Harmonization Guidelines

ITU-T recommends aligning legacy rules with modern frameworks to ensure technological neutrality and consumer benefit.

Thus, consolidation is the international best practice.

5. Consumer Benefits of Regulatory Consolidation

a) Affordability

Removing outdated charging/settlement provisions prevents:

- double-charging,
 - inconsistent recovery mechanisms,
- leading to **lower cost burdens** and improved tariff affordability.

b) Reliability

A unified code eliminates contradictory rules, reducing:

- interconnection disputes,
- POI delays,
- service disruptions.

c) Transparency

Single-point regulation ensures clarity for all stakeholders, enhancing:

- consumer trust,
- accountability,
- non-discriminatory practices.

d) Protection from Anti-Competitive Behavior

Clear, unified rules prevent abuse of dominant positions and ensure:

- fair access,

- transparent charges,
- level playing field.

6. Proposed Methodology for Implementation (A Unified Interconnection Code)

A) Merge Overlapping Provisions

Identify all duplicative or superseded clauses in:

- Section IV,
 - Schedule I (interconnect usage),
 - Schedule II (revenue sharing),
- and consolidate them with the IUC 2003 framework.

B) Create a Unified Interconnection Code

A single, technologically neutral regulation covering:

1. Commercial terms
2. Technical parameters (IP-based)
3. QoS & SLA
4. Security
5. Charges (if any)
6. POI provisioning timelines
7. Anti-fraud obligations
8. Dispute mechanisms

C) Introduce Regulator Dashboards

A TRAI dashboard to:

- monitor compliance,
- publish charge ceilings,
- track interconnection timelines,
- highlight violations.

D) Phased Rollout

1. **Phase 1:** Identification & harmonization of duplicative rules.
2. **Phase 2:** Draft unified interconnection code.
3. **Phase 3:** Industry consultation and finalization.
4. **Phase 4:** Full enforcement with online dashboards.

E) Multilingual Consumer Communication

Public awareness through:

- regional-language summaries,
- digital explainer videos,
- FAQs on interconnection transparency.

This ensures consumer involvement and trust.

7. Conclusion and Justification

The evolution of India’s telecom ecosystem—from TDM to IP, from voice to data, from physical POIs to cloud-native interconnects—renders many provisions of Section IV and Schedules I & II of the 2001 Regulations outdated. The IUC Regulations of 2003 already superseded substantial portions of these provisions, and modern telecom realities now demand **regulatory consolidation**.

A **Unified Interconnection Code**, supported by digital dashboards, standardized parameters, and multilingual transparency measures, aligns India with global best practices (EU, Ofcom, FCC, ITU) while enhancing consumer affordability, service reliability, and protection from anti-competitive behavior.

This consolidation is not only an administrative reform—it is a **consumer-centric necessity in the era of 5G, OTT, cloud communication, and digital transformation**.

Comparison Table: Current vs Proposed Consolidated Interconnection Framework

Aspect	Current Framework (2001 Regulations + 2003 IUC Regulations + Subsequent Amendments)	Proposed Consolidated, Forward-Looking Framework
Regulatory Structure	Fragmented across multiple regulations: 2001 Interconnection (Charges & Revenue Sharing), 2003 IUC, amendments & circulars.	Unified “Interconnection Code of India” integrating 2001 + 2003 + later updates into a single, harmonized regulatory instrument.
Scope of Section IV & Schedules I–II (2001)	Primarily designed for TDM-era cost components (ports, circuits, E1s, physical media). Outdated for IP-based interconnection.	Consolidated technical & financial framework covering IP/SIP-IMS , cloud-native POIs, QoS, routing, security, SBC/ENUM standards.
Technology Base	TDM-centric assumptions: circuit-switched traffic, fixed	Technology-neutral framework incorporating VoIP/VoLTE/VoWiFi, 5G slicing,

Aspect	Current Framework (2001 Regulations + 2003 IUC Regulations + Subsequent Amendments)	Proposed Consolidated, Forward-Looking Framework
	capacity units, physical port charges.	IoT M2M traffic, virtualized interconnects, SDN/NFV.
Traffic Measurement	Legacy measures: MOU, port capacity, circuit provisioning.	AI-driven traffic analytics , QoS dashboards, packet-based measurement, dynamic utilization, and real-time interconnection KPIs.
Interconnection Charges	Based on legacy cost components (port charges & revenue sharing formulas) that overlap with IUC 2003.	Clear, non-overlapping cost-based/zero-rated principles , avoiding duplication with IUC; transparent ceilings for infrastructure charges.
Structure of Schedules I & II	Hardware- and capacity-specific costing tied to TDM equipment, including E1/T1, PCM trunks.	Modernized cost items: virtual sessions, cloud POIs, SBC resources, API-based interconnect functions; updated QoS & security obligations.
Industry Alignment	Misalignment between 2001 schedules and current IP-/cloud-based network design; unnecessary compliance complexity.	Simplified compliance aligned to digital networks, enterprise traffic, CPaaS ecosystem, OTT interconnect models & cloud compute resources.
International Alignment	Lags behind EU, Ofcom, FCC frameworks which emphasize unified, simplified, technology-neutral interconnect rules.	Fully aligned with EU consolidated frameworks , Ofcom SMP simplification , FCC

Aspect	Current Framework (2001 Regulations + 2003 IUC Regulations + Subsequent Amendments)	Proposed Consolidated, Forward-Looking Framework
		unified rules, and ITU-T harmonization guidelines.
Consumer Transparency	Limited visibility; outdated charging constructs do not reflect consumer expectations or modern service patterns.	Dashboard-based disclosure, multilingual consumer education, clarity on costs → better affordability and trust.
Regulatory Monitoring	Manual, document-centric oversight; dependent on inspections or disputes.	Regulator dashboards, automated alerts, real-time performance reporting, compliance analytics.
Treatment of OTT & Enterprise Traffic	Not recognized in 2001 schedules; regulatory vacuum leads to disputes and inconsistent practices.	Explicitly covered: OTT QoS interconnects, CPaaS, enterprise messaging/voice, IoT traffic frameworks, hybrid models.
Grey Route & Fraud Controls	Insufficient provisions for IP fraud, spoofing, smishing/CLI manipulation.	Integrated anti-fraud controls: STIR/SHAKEN-like verification, AI fraud engines, secure routing, encryption mandates, monitoring SLAs.
Consumer Impact	Risk of inflated/duplicative costs; outdated rules cause disputes leading to service disruption and hidden cost burdens.	Lower costs, higher reliability, fewer disputes, and enhanced digital trust through consolidated, predictable interconnection rules.

Justification for the Proposed Consolidated Interconnection Framework

The Indian telecom sector has undergone a transformational shift since the issuance of the Telecommunication Interconnection (Charges and Revenue Sharing) Regulations, 2001. Section IV and Schedules I & II of the 2001 Regulations were designed for a predominantly voice-centric, TDM-based environment. However, with the introduction of the Interconnection Usage Charges (IUC) Regulations, 2003—and more importantly, the transition to digital, IP-centric networks—the original provisions have become partly overlapping, partly redundant, and insufficient to address the complexities of modern interconnection ecosystems. A consolidated, unified framework is therefore indispensable.

Today's network environment is driven by **IP-based interconnection, cloud-native Points of Interconnect (POIs), AI-driven traffic analytics, programmable session border controllers**, and emerging use cases such as **5G slicing, IoT networks, and enterprise-grade OTT communication**. These technologies demand a regulatory structure that is unified, future-ready, and capable of addressing cross-layer interactions. Maintaining two parallel frameworks—the 2001 and 2003 Regulations—creates interpretational inconsistencies, increases compliance burden, and contributes to disputes related to charges, settlement, and obligations. Consolidation will ensure clarity, consistency, and operational efficiency.

Industry realities have equally evolved. India has experienced a near-complete migration from legacy TDM to SIP-IMS and VoLTE/VoWiFi architectures, a surge in A2P/enterprise messaging, and the growth of new business models such as CPaaS, cloud communication, and content-layer

interconnection. Grey-route pressures and sophisticated bypass techniques further demand an integrated regulatory framework that combines financial, technical, and security-related obligations in one place. A unified code eliminates fragmentation and enables rapid regulatory response to emerging threats and market failures.

International best practices strongly support consolidation. The **European Union** has progressively harmonized interconnection rules under the European Electronic Communications Code (EECC), reducing legacy fragmentation. **Ofcom** in the UK has simplified Significant Market Power (SMP) frameworks into unified obligations covering transparency, non-discrimination, and charge control. The **FCC** in the United States applies a cohesive set of interconnection requirements irrespective of underlying technology. **ITU-T guidelines** also emphasize harmonization, predictability, and reduction of regulatory duplication. India's adoption of a similar consolidation approach will reinforce investor confidence, operational efficiency, and regulatory clarity.

Most importantly, **consumers gain immensely** from consolidation. A unified framework increases reliability by ensuring consistent POI provisioning across technologies, reduces costs by eliminating ambiguity and inefficient dispute cycles, enhances transparency of interconnection charges, and safeguards users from anti-competitive behavior. A streamlined regulatory structure ensures that delays, disputes, and inconsistencies in interconnection—one of the chief causes of call drops, poor quality, and service disruptions—are minimized.

The proposed methodology—merging overlapping provisions, creating a unified interconnection code, introducing regulator dashboards, using standardized formats, phasing implementation, and ensuring multilingual public communication—ensures a smooth transition without market disruption. It also promotes long-term stability by aligning India with global best practices and supporting the government’s broader Digital India and 5G/6G readiness goals.

In conclusion, consolidating Section IV and Schedules I & II of the 2001 Regulations with the IUC framework is essential for building a **simplified, future-proof, consumer-centric interconnection regulatory architecture**. This unified approach enhances affordability, strengthens reliability, promotes transparency, and ensures a resilient and competitive telecom environment for India’s digital future.

Q28. Is there a need for change, if any, required in respect of following: i. ii. iii. iv. Port Technology Port Size (Capacity) Port Charges Any other related aspect Kindly provide a detailed response with justification.

Comments : **Yes.**

1. Technology Advancement: Why the Existing Framework Needs Modernization

1.1 Transition from TDM to IP/SIP-IMS Interconnection

India’s interconnection ecosystem is rapidly shifting from legacy TDM/E1 environments to **IP-based SIP/IMS interconnect**, which supports:

- High-definition voice

- Better resiliency
- Direct support for VoLTE, VoWiFi, and 5G voice
- Multimedia-capable sessions including RCS (Rich Communication Services)

Modern interconnection requires **revised port technology specifications** to reflect:

- **SIP-IMS compliant interfaces**
- **Standardized SIP profiles, codecs, and header norms**
- **Mutual authentication and end-to-end security**
- **Programmable Session Border Controllers (SBCs)** capable of dynamic routing

1.2 Cloud-Native, Virtual, and Distributed POIs

Global telecom architectures are moving towards:

- **Virtualized POIs (vPOIs)** running on cloud infrastructure
- **Geo-redundant micro-POIs** with dynamic scaling
- **Edge-based interconnection** for latency-sensitive services

This technological evolution demands **updated port definitions**, enabling:

- On-demand port scaling
- Virtual port allocation
- Software-defined interconnection without physical capacity bottlenecks

1.3 5G Slicing, IoT and Next-Generation Messaging

Modern networks must support:

- **5G network slicing** with different QoS profiles
- **IoT signalling** (low throughput but high reliability)
- **A2P and enterprise messaging**, requiring differentiated interconnection treatment
- **AI/analytics-driven routing** to prevent fraud and improve resilience

This requires **new categories of ports**, including:

- Data-only signalling ports
- IoT/M2M optimized signalling ports
- Low-latency ports for emergency and critical communications

2. Industry Changes Necessitating Revision

2.1 Decline of Legacy Voice/SMS and Rise of IP-Based Traffic

Major transformations shaping interconnection:

- VoLTE and VoWiFi replacing circuit-switched voice
- Explosion in OTT and RCS messaging
- On-demand enterprise traffic (A2P, fintech, telemedicine)
- Increased cross-border ingress (international traffic, roaming, CPaaS platforms)

2.2 Increasing Need for Security and Resilience

Consumers today expect:

- Zero downtime
- Protection from spoofing and spam

- Reliable emergency calling

Industry realities—DDoS risks, surge traffic, disaster scenarios—require ports with:

- Built-in security profiles
- Multi-path redundancy
- AI-based anomaly detection

2.3 Faster Traffic Growth Requires Smarter Capacity Rules

The traditional metric of fixed “ports per Erlang” is no longer relevant in cloud-native, software-defined environments.

Modern networks need:

- Dynamic scaling
- Predictive port planning
- Automated congestion control

Thus, capacity rules must reflect:

- **Peak traffic elasticity**
- **Hourly/daily load variation**
- **Slicing-driven differentiated capacity needs**

3. International Practices Supporting the Need for Change

3.1 ETSI/3GPP SIP Profiles

Europe and global markets use:

- **ETSI TS 102 027** SIP standards

- **3GPP IMS MMTel profiles**
- Mandatory mutual authentication

India must harmonize interconnection port technology with these profiles.

3.2 STIR/SHAKEN for Caller Authentication

Countries like the US and Canada mandate:

- **Caller ID verification**
- Certificate-based call signing
- End-to-end identity protection

Port technology must embed support for:

- Authentication tokens
- Secure identity headers
- Anti-spoofing validation

3.3 Ofcom/EU QoS, Transparency, and Reporting Rules

International regulators require:

- Clear QoS SLAs
- Mandatory network analytics reporting
- Consumer transparency dashboards

India's port sizing and SLA rules must align with these norms.

3.4 NG-112 and NG-911: Next-Generation Emergency Routing

Modern emergency frameworks require:

- SIP-based location routing
- High-availability redundant ports
- Priority call treatment

Indian interconnection must integrate similar safeguards to protect consumer safety.

4. Consumer Benefits from Revising Ports & Interconnection Framework

4.1 Affordability

- Cost-based port charges remove hidden costs
- Virtual ports reduce CAPEX → lower tariffs
- Efficient routing minimizes congestion and drops

4.2 Reliability

- Geo-redundant and cloud-native ports ensure uptime
- Elastic capacity avoids busy-hours and call failures
- AI-based anomaly detection prevents network breakdowns

4.3 Trust & Safety

- STIR/SHAKEN-compatible ports reduce spoofing and spam
- Secure SIP headers protect user identity
- Verified emergency routing improves life-saving response

4.4 Better Digital Experience

Consumers benefit from:

- HD voice (VoLTE/VoWiFi)
- Reliable A2P verifications (banking OTPs, UPI alerts)
- Seamless connectivity across 5G, IoT, and apps

5. Proposed Methodology for Implementation

5.1 Revision of Technology Profiles

TRAI may update interconnection norms to include:

- Mandatory **SIP-IMS compliance**
- Support for **STIR/SHAKEN-like authentication**
- Role of SBCs in security, analytics, and QoS
- Cloud-native POI definitions

5.2 Modern Port Capacity Planning Rules

Replace legacy fixed port rules with:

- **Elastic and virtual port allocation**
- Predictive AI-driven capacity forecasting
- Mandatory redundancy levels (e.g., N+1, geo-redundant)

5.3 Cost-Based Port Charging & Consumer-Friendly Ceilings

Port charges should be:

- Cost-based
- Transparency-driven
- Subject to maximum ceilings
- Differentiated for virtual vs physical ports
- Linked to utilization efficiency

5.4 Telemetry-Driven SLAs and Dashboards

Mandate real-time reporting on:

- Utilization
- Call drop rates
- Packet loss/jitter
- Fraud attempts blocked
- Emergency call success rate

Dashboards should be accessible to:

- Regulator
- Consumers (summary form)
- Academia/industry bodies

5.5 Phased Rollout

- Phase 1: New interconnections on SIP-IMS
- Phase 2: Legacy ports migrate gradually
- Phase 3: Cloud/virtual POIs and STIR/SHAKEN-like authentication
- Phase 4: Unified emergency routing readiness

5.6 Multilingual Consumer Communication

Essential to build public trust, including:

- FAQs
- Public advisories
- Safety instructions
- Dashboard summaries

- Infographics on fraud prevention

6. Conclusion: Why Changes Are Necessary

Revising port technology, size, charges, and related interconnection aspects is essential to ensure that India's telecom ecosystem remains:

- **Consumer-Centric**

Offering reliable, affordable, secure, and high-quality services.

- **Future-Ready**

Supporting VoLTE/VoWiFi, 5G, M2M, A2P messaging, and next-generation emergency services.

- **Globally Harmonized**

Aligned with ETSI/3GPP SIP profiles, Ofcom/EU transparency rules, STIR/SHAKEN authentication, and NG-112/NG-911 emergency frameworks.

- **Competition-Friendly**

Eliminating bottlenecks, encouraging innovation, and enabling efficient interconnection.

These changes protect consumers, enhance service reliability, support digital inclusion, and position India's telecom sector as a global leader.

Below is a **clear, structured, and regulator-grade comparison table** of the **Current vs Proposed Interconnection Framework**, aligned with your detailed response.

Comparison Table: Current vs Proposed Interconnection Framework

Parameter	Current Interconnection Framework	Proposed Future-Ready Interconnection Framework
1. Port Technology	<ul style="list-style-type: none"> Primarily TDM/E1, SS7 signalling Limited SIP interconnect use Hardware-based POIs 	<ul style="list-style-type: none"> SIP-IMS mandatory for all new interconnections Support for secure SIP headers, HD voice, VoLTE/VoWiFi Cloud-native / virtual POIs (vPOIs) using NFV/SDN Integrated programmable SBCs for routing, security, analytics
2. Port Capacity / Sizing	<ul style="list-style-type: none"> Physical port count linked to Erlangs Static capacity, slow scaling Minimal redundancy (often single-path) 	<ul style="list-style-type: none"> Elastic, on-demand port scaling (virtual ports) AI-based predictive capacity planning Mandatory redundancy (N+1, geo-redundant) Slicing-based differentiated capacity for IoT, emergency, enterprise
3. Port Charges	<ul style="list-style-type: none"> Port charges depend on physical infrastructure CAPEX-heavy model No clear ceilings for consumer protection Varied treatment across operators 	<ul style="list-style-type: none"> Cost-based port charge methodology Ceiling-based tariffs to prevent overcharging Transparent, uniform charging frameworks Lower costs due to virtual ports + reduced CAPEX
4. Security / Authentication	<ul style="list-style-type: none"> Limited caller authentication Vulnerable to spoofing, grey routes Basic signalling validation 	<ul style="list-style-type: none"> STIR/SHAKEN-like authentication for caller identity Quantum-safe and certificate-based security Real-time fraud analytics integrated at ports Strong mutual authentication between networks

Parameter	Current Interconnection Framework	Proposed Future-Ready Interconnection Framework
5. Resilience & Redundancy	<ul style="list-style-type: none"> • Manual failover; single physical POI often a bottleneck • Outages impact large consumer groups • Minimal telemetry 	<ul style="list-style-type: none"> • Geo-redundant virtual POIs Automated failover and load shifting Real-time health monitoring of interconnect links • AI-driven anomaly detection for outages and DDoS
6. Emergency Call Handling	<ul style="list-style-type: none"> • Legacy routing for 100/101/102 • Limited location information • No priority handling 	<ul style="list-style-type: none"> • NG-112 / NG-911 compliant routing Location-based SIP emergency routing • Guaranteed priority access and fallback paths • Specialized emergency-grade SIP profiles
7. Support for Modern Services	<ul style="list-style-type: none"> • Optimized mainly for voice/SMS traffic • OTT/A2P often treated indirectly • Limited support for IoT/5G/edge services 	<ul style="list-style-type: none"> • Full support for 5G slicing, VoLTE, VoWiFi, RCS • Dedicated interconnect profiles for A2P, fintech, telemedicine • IoT-friendly signalling interfaces • Edge-based distributed interconnection
8. Monitoring, QoS & SLAs	<ul style="list-style-type: none"> • Reactive monitoring • Key metrics: call drops, ASR, congestion • Limited transparency to consumers 	<ul style="list-style-type: none"> • Telemetry-driven SLAs with real-time metrics • Port-wise monitoring of jitter, latency, packet loss • Public consumer transparency dashboards (multilingual) • Live fraud-blocking counters
9. Regulatory Compliance	<ul style="list-style-type: none"> • Framework split between multiple legacy regulations • Non-uniform 	<ul style="list-style-type: none"> • Unified IP-based Interconnection Code simplifying all rules • Harmonized SIP profiles, security, and capacity rules • Standardized

Parameter	Current Interconnection Framework	Proposed Future-Ready Interconnection Framework
	implementation• Overlapping obligations	reporting formats & real-time dashboards
10. Consumer Experience	<ul style="list-style-type: none"> • Occasional call failures during congestions • Uncertain identity of callers (spoofing/spam) • Lower quality for cross-network calls 	<ul style="list-style-type: none"> • HD voice and seamless cross-network quality • Strong identity protection → fewer fraud calls • Lower outages, faster call setup • Transparent routing & safety mechanisms
11. Suitability for Future Growth	<ul style="list-style-type: none"> • Not compatible with full-scale 5G and IoT • High operational cost • Inflexible 	<ul style="list-style-type: none"> • Designed for 5G, IoT, AI-driven networks • Scalable, flexible, cloud-native • Encourages innovation and fair competition

Summary: Why the Proposed Framework is Superior for Consumers

The proposed interconnection framework ensures:

- ✓ **Higher reliability:** through geo-redundancy, automation, and elastic scaling
- ✓ **Better affordability:** cost-based charging + virtual ports
- ✓ **Enhanced safety:** STIR/SHAKEN-like authentication + NG emergency routing
- ✓ **Improved digital experience:** VoLTE/VoWiFi HD voice + RCS + IoT
- ✓ **Increased transparency:** real-time dashboards and QoS reporting
- ✓ **Future readiness:** aligned with 5G, edge computing, and global standards

This framework places **consumer protection, fair competition, and global alignment** at the center of interconnection modernization.

Justification for the Proposed Interconnection Framework :

The comparison between the current and proposed interconnection frameworks clearly demonstrates that modernization is essential to protect consumer interests, ensure reliability, and align India's telecom ecosystem with global best practices. The existing framework—designed around legacy TDM/E1, static port capacity, and hardware-dependent POIs—has reached its operational and technological limits in a rapidly evolving environment defined by 5G, VoLTE/VoWiFi, cloud services, A2P/OTT traffic growth, cybersecurity threats, and rising consumer expectations.

1. Technology Modernization for Quality and Reliability

The shift toward SIP-IMS, programmable SBCs, and cloud-native/virtual POIs is no longer optional. Modern communication networks—5G slices, IoT signalling, RCS messaging, and emergency routing—cannot function optimally on legacy TDM interfaces. Updated port technology enables higher quality (HD voice), faster call setup times, improved interoperability, and seamless cross-network connectivity. This directly improves consumer experience, reduces call failures, and enhances service reliability.

2. Elastic Capacity and Redundancy for Consumer Safety

Static port sizing based on fixed Erlang estimates cannot cope with today's dynamic and bursty traffic patterns. Elastic virtual ports, predictive capacity planning, and geo-redundant interconnection prevent congestion, reduce outages, and ensure continuity during disasters or cyber incidents.

Consumers benefit from lower call drops, fewer busy hours, and uninterrupted access to emergency services.

3. Security and Identity Protection for Consumer Trust

Rapid growth in fraud, spoofing, and grey-route manipulation requires port technology to incorporate modern authentication standards. STIR/SHAKEN-like mechanisms, secure SIP headers, and SBC-embedded analytics significantly reduce fraudulent calls and safeguard consumer identity. Strengthening interconnection security is essential to restore trust in digital communications and support critical services such as banking, UPI, telemedicine, and e-governance.

4. Cost-Based Charges Ensure Fairness and Affordability

Port charges in the current framework reflect physical infrastructure and legacy cost models. Virtual ports and cloud-native POIs substantially lower CAPEX/OPEX requirements, enabling cost-based charges and tariff ceilings that protect consumers from hidden or inflated interconnection costs. Transparent, uniform charging frameworks promote competition and prevent discriminatory practices.

5. International Alignment for Global Competitiveness

Leading regulators—Ofcom, ETSI, FCC, EU authorities—have already adopted IP-based interconnection profiles, secure caller ID frameworks, telemetry-driven QoS reporting, and NG-112/911 emergency routing. Aligning Indian regulations with these norms ensures interoperability, enhances the global credibility of Indian networks, and prepares the ecosystem for cross-border digital services and future innovations.

6. Transparency and Accountability Through Telemetry & Dashboards

Modern networks enable real-time measurement of jitter, latency, packet loss, emergency call success rates, and fraud-blocking statistics. Mandating telemetry-driven SLAs and public dashboards fosters accountability and empowers consumers with clear, multilingual information on network performance—an essential pillar of consumer protection.

Conclusion

Modernizing the interconnection framework—covering port technology, capacity rules, charges, and related aspects—is essential not merely for technical efficiency but for **consumer protection, safety, trust, and affordability**. The proposed framework ensures resilient, secure, transparent, and future-ready networks fully aligned with global standards, enabling India to deliver world-class communication services to every consumer while supporting innovation, competition, and national digital transformation.

Q29. Should port charges be uniform across all services and technologies? Kindly provide detailed response for the following categories specifically: a. Fixed Line Service/ Mobile Service/ NLD service/ ILD service, and b. E1 (TDM) based interconnection and IP based interconnection. 139 In case non-uniform charges are suggested, what methodology should be followed for calculation of port charges for above mentioned categories of services and technologies. Kindly provide a detailed response with justification.

Comments :

1. Position in Brief

Port charges **should follow common, technology-neutral and non-discriminatory principles**, but **need not be strictly identical in rupee terms** across:

- a) fixed line, mobile, NLD, ILD; and
- b) E1 (TDM) vs IP-based interconnection.

Instead, the framework should be:

- **Cost-based and transparent,**
- **Technology-neutral in principle, but**
- Allowing **differentiated classes of ports** (e.g., legacy TDM, SIP/IMS, virtual/ cloud ports, emergency/special QoS ports) with **justified cost differentials**, subject to **regulatory ceilings** and strict **non-discrimination** between similarly placed operators.

This approach maximizes **consumer welfare, affordability, reliability, and fair competition**.

2. Technology Advancement: Why “One-Size-Fits-All” Is Not Optimal

2.1 SIP/IMS and Cloud-Native / Virtual POIs

Modern interconnection based on **SIP/IMS, cloud-native POIs** and **virtual ports** has very different cost and performance characteristics compared to legacy **E1/TDM** ports:

- **TDM/E1 ports:** hardware-bound, limited scalability, higher incremental CAPEX/OPEX.
- **IP/SIP-IMS ports:** software-defined, elastic, shareable across multiple services (fixed, mobile, NLD, ILD) and can be hosted on **virtualized infrastructure**.
- **Programmable SBCs,** AI-driven observability and 5G slicing allow dynamic control of security, QoS and routing at the port level.

It would be **inefficient and distortionary** to force identical port charges across completely different cost structures. However, **within the same technology class** (e.g. IP interconnect ports across fixed and mobile, or virtual ports across services), **charges must be uniform and non-discriminatory**.

2.2 5G Slicing and Differentiated QoS

5G network slicing and rich communication services (RCS) require:

- Different QoS profiles (eMBB, URLLC, mMTC).
- Higher reliability and ultra-low latency for some ports (e.g., emergency, critical IoT, telemedicine).

Ports that support **specialized slices with strict QoS and redundancy** may legitimately have a different cost base than standard best-effort ports, but this must be **transparent, cost-justified and regulated**.

3. Industry Changes: Legacy-to-IP Migration and New Demands

3.1 Mixed Traffic Environment (Fixed, Mobile, NLD, ILD)

Port usage now spans:

- Traditional voice on fixed and mobile,
- **NLD/ILD voice and signalling,**
- **A2P/enterprise traffic,**
- OTT interconnect and cross-border ingress,
- IoT/VoWiFi/VoLTE, rich multimedia sessions.

A rigid, uniform port charge across all services risks:

- Over-recovery in low-cost IP environments,
- Under-recovery where legacy infrastructure must be maintained temporarily,
- Distorted incentives to migrate to IP and to invest in resilience and security.

A **service-agnostic but cost-aligned structure** is better: the same IP port (or class of virtual ports) should carry fixed, mobile, NLD, and ILD traffic without different prices **for the same resource**. Any differentiation should be based on **objectively different resources or QoS requirements, not on service labels**.

3.2 Resilience, Security and AI-Based Management

The industry is also facing:

- Higher expectations on **resilience** (disasters, surges, cyber incidents).
- Need for **AI-driven anomaly detection** and continuous security analytics at interconnection points.

Where operators invest in **mandatory regulator-specified resilience/security capabilities** at ports, these will influence cost. The framework must allow **recovery of justified additional cost**, but under **common rules** applicable to all operators.

4. International Practice: Cost-Based, Transparent, and Tech-Aligned

Internationally:

- **ETSI/3GPP** define **SIP/IMS profiles** and QoS parameters suitable for converged fixed–mobile–NLD–ILD interconnect on IP.
- **Ofcom and EU regulators** favour **cost-based, transparent** interconnection charges with strong non-discrimination and technology-neutrality at the principle level, not uniform rupee values across all technologies.
- **STIR/SHAKEN** frameworks integrate caller authentication at the interconnection layer; adding such capabilities alters cost but increases consumer trust.
- **NG-112/NG-911** emergency architectures require priority routing and geo-redundant capacity, again creating specific port classes with enhanced requirements.

The consistent theme is:

Uniform principles (cost orientation, transparency, non-discrimination, tech neutrality) with **flexible, justified differentiation** where technology and QoS genuinely differ.

India's framework should mirror this.

5. Consumer Benefits: How the Right Port Charge Design Helps

5.1 Affordability

- **Cost-based and efficiency-reflective charges** for IP/virtual ports will **reduce overall cost of interconnection**, and thereby lower end-user tariffs.
- Avoiding excessive or service-biased port charges prevents anti-competitive costs being passed on to consumers (e.g., higher ILD or NLD charges without cost basis).

5.2 Reliability and Quality

- A framework that **rewards efficient IP migration** and **resilience investments** ensures fewer call drops, better voice quality, and more stable connectivity across fixed, mobile, NLD, and ILD.

5.3 Trust and Safety

- Supporting STIR/SHAKEN-like authentication and NG emergency routing through appropriate port classes improves caller ID trust, reduces spam and fraud, and safeguards life-critical communications.

In all cases, **fair and properly structured port charges** encourage operators to invest in technologies that directly benefit the consumer without fear of being under- or over-compensated.

6. Methodology: How Port Charges Should Be Structured

A consumer-centric, forward-looking framework should follow these principles:

1. **Cost-Based and Technology-Neutral at the Principle Level**

- Use **long-run incremental cost (LRIC)/cost-plus** methods for both E1/TDM and IP ports.
- Principles apply equally across fixed, mobile, NLD, ILD; no arbitrary mark-ups per service label.

2. **Differentiated Classes of Ports (But Non-Discriminatory Within Each Class)**

- Example classes:
 - Legacy **E1/TDM** ports (time-bound, sunset trajectory)
 - Standard **IP/SIP-IMS** ports
 - **Virtual/cloud-based** ports
 - **Emergency/special QoS** ports (NG-112/NG-911 style)
- Within each class, charges must be **uniform and non-discriminatory** across all TSPs and services.

3. **Ceilings and Guardrails**

- TRAI may prescribe **maximum charge ceilings** for each port class.
- Operators may set lower charges but not exceed ceilings, to protect consumers and smaller operators.

4. **Indexation and Periodic Review**

- Apply transparent **indexation rules** (e.g., linked to WPI/CPI or technology cost indices).
- Periodic review cycles to reflect falling IP/virtualization costs and rising security/resilience obligations.

5. **Transparency, Dashboards, and Reporting**

- Mandate **public dashboards** summarizing: port capacity, utilization, outages, fraud blocked, QoS, and charge levels (in anonymized or banded form).
- This builds consumer confidence and enables informed policy oversight.

6. Phased Rollout and Legacy Protection

- Phase 1: Apply uniform principles immediately; maintain existing E1 charges but freeze or cap them.
- Phase 2: Introduce defined IP/virtual port classes with cost-based ceilings; promote migration.
- Phase 3: Gradually sunset E1/TDM port classes, with clear timelines.

7. Multilingual Consumer Communication

- Explain, in simple language and regional languages, that reforms in interconnection charges are designed to **improve call quality, reduce spam, and lower costs**, not to burden consumers.

7. Conclusion: Clear Justification

Port charges **should not be blindly uniform** across fixed, mobile, NLD, ILD, or across E1 and IP, because the underlying technologies, cost structures, and QoS capabilities are different. However, they **must be governed by uniform principles** of:

- **Cost-based, efficient pricing,**
- **Technology-neutral rules,**
- **Non-discrimination within each port class,**

- **Transparent ceilings and reporting, and**
- **Strong consumer-protection safeguards.**

Such a framework:

- Encourages **timely migration from TDM to IP/virtual interconnection;**
- Promotes **fair competition** among all TSPs;
- Supports **innovation** (5G, IoT, RCS, secure caller ID); and
- Maximizes **consumer benefits in affordability, reliability, trust, and safety.**

Therefore, **TRAI should adopt a cost-based, class-differentiated, but principle-uniform port charge framework rather than a rigid, one-rate-for-all model**, placing consumer protection and fair competition at the core of interconnection policy.

Q30. Whether use of ‘Erlang’ as a unit of traffic in various interconnection regulations is sufficient and are the current procedures for demand estimation as provided in the Telecommunication Interconnection (Port Charges) Regulation 2001 and the TIR 2018 still effective and practical, in view of adoption of IP based interconnection?
a. If yes, kindly provide justification in support of your response. b. If no, kindly provide alternate metrics and demand estimation methods for IP-based interconnection along with detailed explanation. In either case, kindly provide suitable diagrammatic representation. A.9. The Register of Interconnect Agreements Regulations, 1999.

Comments :

1. Technology Advancement: Why Erlang Alone Is No Longer Sufficient

1.1 SIP/IMS Interconnection and Multi-Dimensional Traffic

Interconnection today is dominated by **SIP/IMS**, supporting:

- HD Voice (AMR-WB),
- VoLTE/VoWiFi,
- RCS messaging,
- Rich signalling across SBCs.

Unlike TDM voice trunks, SIP/IMS traffic cannot be accurately captured through a **single scalar unit (Erlang)**. It varies across:

- Concurrent SIP sessions,
- Session establishment rate (Calls Per Second – CPS),
- Codec bandwidth,
- Retransmissions,
- Signalling bursts.

1.2 Cloud-Native POIs & Virtual Interconnects

Modern interconnection involves:

- **Virtual/Cloud-native POIs (vPOIs)**,
- Auto-scaling resources,
- Traffic-aware routing,
- SDN/NFV-based programmable capacity.

These architectures scale elastically and **do not rely on fixed port/E1 capacity**, rendering Erlang insufficient for dimensioning.

1.3 5G, IoT, Slicing, and Real-Time Telemetry

5G supports **URLLC, mMTC, and eMBB slices**, each with distinct traffic patterns and QoS requirements.

IoT uses:

- Short bursts,
- Low bandwidth,
- High reliability signalling.

IP networks also provide **real-time telemetry** (jitter, latency, loss) unavailable in TDM. Demand estimation must evolve to include such metrics.

2. Industry Changes: Why the Old Methodology (Port Charges Regulations 2001, TIR 2018) Must Evolve

2.1 Migration from TDM/E1 to IP

Most operators have transitioned large parts of interconnection from E1 circuits to SIP trunks. Therefore:

- **Erlang = relevant only for legacy TDM voice,**
- **IP = multidimensional, elastic, bursty traffic.**

2.2 Traffic Mix Has Radically Changed

The traffic ecosystem now includes:

- VoLTE/VoWiFi voice,
- OTT voice/video,
- A2P and CPaaS traffic,

- IoT signalling,
- Cross-border ingress,
- Authentication/OTP traffic requiring ultra-high reliability.

These cannot be captured meaningfully by Erlang alone.

2.3 Resilience & Security Requirements Require New Metrics

Interconnection points must now withstand:

- DDoS attacks,
- Flash crowds,
- Spam bursts,
- Emergency traffic spikes.

Capacity planning requires metrics such as:

- **Peak CPS for SIP floods,**
- **SBC CPU/RAM utilization,**
- **Packet loss thresholds,**
- **Traffic percentiles (P95, P99).**

3. International Practice: Global Regulators Have Moved Beyond Erlang

3.1 ETSI/3GPP SIP Profiles Govern Interconnection

ETSI TS 102 027, 3GPP TS 24-series define capacity in terms of:

- Concurrent SIP dialogs,
- Bandwidth per codec,
- CPS,
- QoS metrics—not Erlangs.

3.2 FCC/Ofcom Reporting

US and UK regulators require:

- Real-time QoS reporting,
- IP traffic analytics,
- Latency/jitter/loss metrics,
- MOS (Mean Opinion Score) measurements.

None rely on Erlang for SIP-IMS networks.

3.3 STIR/SHAKEN Authentication

Authentication adds:

- Crypto overhead,
- Additional signalling bursts,
- Token processing.

These require **SIP session-rate** and **processing load** metrics, not Erlangs.

3.4 NG-112/NG-911 Emergency Frameworks

Interconnection dimensioning includes:

- Priority routing,
- Geo-redundancy metrics,
- Packet-level QoS.

Again, metrics are IP-native.

4. Consumer Benefits of a Modern Demand-Estimation Framework

4.1 Affordability

Using accurate, IP-native dimensioning:

- Prevents over-provisioning,
- Reduces interconnection cost,
- Ensures lower tariffs and better value.

4.2 Reliability & Quality

Real-time telemetry and percentile-based capacity ensure:

- Minimal congestion,
- Fewer call drops,
- Stable VoLTE/VoWiFi quality,
- Reliable OTP/A2P delivery.

4.3 Transparency

IP metrics provide clarity on:

- Network behaviour,
- Service quality,
- Routing integrity.

Dashboards make this transparent for consumers.

4.4 Protection from Fraud/Spam

SIP-level analytics enable:

- Early detection of spam bursts,
- Blocking spoofed traffic,

- Prioritization of emergency traffic.

Consumers experience safer and more trustworthy communication.

5. Recommended Methodology: Hybrid Erlang/IP Demand Estimation

5.1 Retain Erlang for Legacy TDM Voice

Wherever E1/TDM ports remain (in sunset phase),

Erlang continues as the correct unit.

5.2 Adopt IP-Native Metrics for SIP/IMS Interconnection

The regulator should define minimum metrics for all new interconnects:

1. **Concurrent Sessions** (channels equivalent)
2. **Calls Per Second (CPS)**
3. **Bandwidth / Throughput** (Mbps/Gbps)
4. **Latency / Jitter / Packet Loss** thresholds
5. **MOS score**
6. **P95/P99 percentile utilisation**
7. **SBC resource utilisation** (CPU/RAM)
8. **Fraud/spam detection counters**

5.3 Percentile-Based Demand Forecasting

Move from average traffic calculations to:

- **95th percentile,**
- **99th percentile,**
- **Peak hour traffic variability.**

5.4 Regulators' Dashboards & Real-Time Monitoring

TRAI may require operators to publish:

- Interconnection health indicators,
- Demand forecasts,
- Congestion alerts,
- Spam/fraud blocks,
- Emergency call success rates.

5.5 Phased Rollout

Phase 1 – Keep Erlang for TDM; start collecting SIP/IP metrics

Phase 2 – Use hybrid model for all IP-based ports

Phase 3 – Sunset Erlang as TDM retirements complete

Phase 4 – Fully IP-native framework

5.6 Multilingual Consumer Communication

Explain in simple Indian languages how modern metrics enhance:

- Call quality,
- Security,
- Emergency services,
- Digital trust.

6. Conclusion: Clear Consumer-Centric Justification

Erlang is **adequate only for legacy TDM/E1 voice**.

In today's **IP-based, SIP/IMS-driven, multi-service, elastic, cloud-native** ecosystem, a **hybrid Erlang/IP framework** is essential.

This approach:

- ✓ Preserves continuity for legacy systems
- ✓ Enables accurate forecasting for modern IP traffic
- ✓ Supports 5G/IoT, OTT, A2P, and secure communications
- ✓ Ensures affordability through efficient provisioning
- ✓ Enhances reliability, emergency readiness, and fraud protection
- ✓ Aligns India with ETSI/3GPP, FCC, Ofcom, and global best practices

Thus, **Erlang must transition from being the primary metric to being one component of a modern, multi-metric, IP-native demand-estimation system—anchored in consumer protection, reliability, and transparency.**

Comparison Table: Current vs Proposed Traffic Measurement Framework

Parameter	Current Framework (Erlang + Legacy Methods)	Proposed Framework (Hybrid Erlang + IP-Native Metrics)
1. Traffic Unit / Measurement Basis	<ul style="list-style-type: none">• Erlang is the primary unit.• Assumes constant, circuit-switched voice traffic.• Suitable for E1/TDM trunks only.	<ul style="list-style-type: none">• Hybrid model: Erlang for legacy TDM + IP-native metrics for SIP/IMS.• Metrics include concurrent sessions, CPS, throughput, jitter, latency, loss, MOS, telemetry signals.
2. Applicable Technologies	<ul style="list-style-type: none">• Works only for circuit-switched voice.• Does not reflect IP/SIP traffic diversity.	<ul style="list-style-type: none">• Supports VoLTE/VoWiFi, SIP trunking, cloud-native POIs, multi-codec voice, RCS messaging, and IoT/5G slices.• Accommodates

Parameter	Current Framework (Erlang + Legacy Methods)	Proposed Framework (Hybrid Erlang + IP-Native Metrics)
		elastic capacity and multi-service flows.
3. Network Architecture Assumption	<ul style="list-style-type: none"> • Static, hardware-based physical ports (E1). • Predictable, uniform call behavior. 	<ul style="list-style-type: none"> • Cloud-native / virtual POIs, elastic scaling, SDN/NFV, and programmable SBCs. • Traffic is bursty, multi-dimensional, and service-specific.
4. Demand Estimation Method	<ul style="list-style-type: none"> • Average Erlang calculations. • Limited capacity to track bursts. 	<ul style="list-style-type: none"> • Percentile-based forecasting (P95, P99). • AI-driven predictive analytics. • Session-rate and bandwidth forecasting.
5. Traffic Types Considered	<ul style="list-style-type: none"> • Mainly voice (fixed/mobile). • No native support for OTT/A2P/IoT. 	<ul style="list-style-type: none"> • Multi-service model: VoLTE, VoWiFi, OTT, A2P/CPaaS, IoT, emergency sessions. • Recognizes multimedia signalling and security loads.
6. Real-Time Observability	<ul style="list-style-type: none"> • Minimal real-time insight. • Uses historical call patterns. 	<ul style="list-style-type: none"> • Full telemetry: jitter, latency, loss, MOS, congestion alerts, SBC analytics. • Real-time programmable routing decisions.
7. Security / Authentication Load	<ul style="list-style-type: none"> • No integration with security analytics. • No capacity for STIR/SHAKEN-like validation. 	<ul style="list-style-type: none"> • Supports STIR/SHAKEN, SIP identity verification, anomaly detection, spam/fraud bursts. • Traffic includes crypto and security overhead.
8. Emergency Traffic (NG-	<ul style="list-style-type: none"> • Same treatment as normal calls. • No priority routing metrics. 	<ul style="list-style-type: none"> • Dedicated metrics for emergency routing. • Priority flows, ultra-low latency, geo-redundant traffic

Parameter	Current Framework (Erlang + Legacy Methods)	Proposed Framework (Hybrid Erlang + IP-Native Metrics)
112/NG-911 readiness)		paths. • Capacity calculated by reliability need.
9. Burst Traffic Handling (A2P/OTP surges)	<ul style="list-style-type: none"> • Not designed for large signalling bursts. • Leads to congestion under spikes. 	<ul style="list-style-type: none"> • Uses CPS (Calls Per Second), transaction-per-second metrics, signalling load estimation. • Ensures reliable OTP delivery and spam filtering.
10. Scalability Approach	<ul style="list-style-type: none"> • Physical ports need manual expansion. • Slow and costly. 	<ul style="list-style-type: none"> • Elastic scaling of virtual ports. • Auto-scaling triggers based on load, telemetry, and AI models.
11. Transparency & Reporting	<ul style="list-style-type: none"> • Limited reporting; not consumer-friendly. • No real-time dashboards. 	<ul style="list-style-type: none"> • Real-time dashboards showing QoS, congestion, spam-blocking, session load (multilingual summaries).
12. Regulation & Compliance Fit	<ul style="list-style-type: none"> • Based on Port Charges Regulation, 2001 & TIR 2018. • Increasingly misaligned with IP-era demands. 	<ul style="list-style-type: none"> • Fully aligned with global standards (ETSI/3GPP SIP profiles, FCC/Ofcom QoS norms). • Future-ready for 5G, IoT, and cloud interconnects.
13. Consumer Impact	<ul style="list-style-type: none"> • Occasional congestion, unreliable OTP delivery, variable VoLTE quality. • Less protection from spam/fraud. 	<ul style="list-style-type: none"> • Higher reliability, stable VoLTE/VoWiFi quality, improved OTP delivery, spam/fraud protection. • Greater transparency and safety.

Summary: Why the Proposed Framework Is Better for Consumers

✓ Accurate Measurement

IP-native metrics reflect real user experience (latency, jitter, MOS).

✓ **Improved Reliability**

Elastic scaling + percentile-based forecasting reduces congestion.

✓ **Better Security**

Supports spam detection, STIR/SHAKEN authentication, fraud prevention.

✓ **Future-Proofing**

Ready for VoLTE/VoWiFi, OTT, A2P, IoT, edge traffic, and 5G slicing.

✓ **Consumer Transparency**

Dashboards give visible accountability and trust.

✓ **Alignment with Global Best Practices**

ETSI/3GPP SIP profiles, FCC/Ofcom QoS templates, NG-112/911 metrics.

Justification for the Proposed Traffic Measurement Framework

The existing traffic measurement framework—centered primarily around **Erlang** as the unit of traffic and legacy procedures from the **Port Charges Regulation 2001** and **TIR 2018**—was designed for a circuit-switched, TDM/E1 era where call behavior was predictable, uniform, and voice-centric. In today’s rapidly evolving IP-based environment, this framework is no longer adequate to ensure **reliability, affordability, transparency, and consumer protection**.

1. Technological Evolution Makes Erlang Alone Insufficient

Modern networks operate on **SIP/IMS interconnection, cloud-native/virtual POIs, programmable SBCs, AI-driven traffic analytics, and 5G slicing**. Traffic today varies in dimensions such as:

- Concurrent SIP sessions
- Calls per second (CPS)
- Bandwidth/throughput
- Retransmission spikes
- Multi-codec behaviour
- Real-time telemetry (latency, jitter, packet loss)

These metrics cannot be captured meaningfully by a **single scalar unit (Erlang)**. While Erlang remains relevant for residual TDM interconnects, IP traffic requires a richer, multi-metric measurement framework.

2. Industry Changes Demand a Modern Approach

India's telecom ecosystem has shifted from predictable, circuit-switched voice to dynamic IP-based traffic comprising:

- VoLTE and VoWiFi
- OTT voice/video
- A2P/CPaaS traffic
- IoT and device signalling bursts
- Real-time emergency traffic
- Cross-border ingress traffic

Elastic demand patterns, resilience requirements (DDoS, spoofing, flash crowds), and 24×7 reliability expectations mean that **average Erlang-based estimation leads to under-provisioning, congestion, or unreliable services**, especially during OTP peaks or emergency situations.

3. Global Best Practices Have Moved Beyond Erlang

International regulators and standards bodies such as **ETSI/3GPP, Ofcom, FCC**, and **NG-112/NG-911** frameworks use:

- Concurrent session measurements
- CPS
- Codec-level bandwidth analysis
- Percentile-based utilization (P95/P99)
- MOS quality metrics
- Real-time QoS/telemetry reporting

No major regulator depends solely on Erlang for IP-based networks. To stay globally aligned and future-ready, India's framework must adopt similar IP-native metrics.

4. Consumer Benefits Strongly Support the Transition

A modern measurement framework directly enhances consumer welfare:

- **Affordability:** Accurate estimation reduces over-provisioning cost and prevents inflated interconnection charges.
- **Reliability:** Fewer call drops, smoother VoLTE/VoWiFi, and stable OTP delivery.

- **Transparency:** Real-time QoS dashboards increase public trust and regulatory accountability.
- **Safety:** Improved emergency routing, fraud/spam mitigation, and caller-ID authentication (STIR/SHAKEN readiness).

5. A Balanced, Hybrid Method Protects Both Continuity and Innovation

The proposed framework is **evolutionary, not disruptive**:

- Retain **Erlang** for legacy TDM networks during their sunset phase.
- Adopt IP-native metrics (concurrent sessions, CPS, jitter/latency/loss, MOS, P95/P99 load, SBC resource utilization) for SIP/IMS interconnect.
- Use AI-assisted forecasting and telemetry-driven dashboards for real-time visibility.
- Implement change through a phased rollout with multilingual consumer communication.

Conclusion

Modernizing traffic measurement from a **Erlang-only** model to a **hybrid Erlang + IP-native multi-metric framework** is essential to protect consumers, ensure high-quality services, and prepare the Indian telecom ecosystem for next-generation networks. This approach aligns with global best practices, supports fair competition, enhances transparency, improves reliability, strengthens digital security, and ensures that consumers receive the full benefits of the digital communications revolution.

Such reform is not just technical—it is a **consumer protection imperative**.

Q31. Should the current provisions for submission, inspection and getting copies of interconnection agreements under ‘The Register of Interconnect Agreements Regulations, 1999’ using floppy disks and print copies be dispensed with and be made online? a. If yes, what changes do you suggest for the online process, timelines, related charges and any other aspect? b. If not, kindly provide justification. B. Generic Questions pertaining to all existing interconnection regulations.

Comments :

Online Replacement of the 1999 Interconnection Register Provisions

Introduction

The current provisions under the *Register of Interconnect Agreements Regulations, 1999*—requiring submission of interconnection agreements through **floppy disks, print copies, and manual inspection procedures**—are no longer aligned with today's digital ecosystem, IP-based networks, hybrid service models, and the need for real-time regulatory oversight. To protect consumers in the era of **5G, cloud, OTT, enterprise messaging, and converged networks**, a **secure, online, transparent, and analytics-enabled system** is essential.

This response assesses why legacy mechanisms should be **dispensed with** and replaced by a **modern digital platform**.

1) Technology Advancement

a) Secure Digital Portals

A regulator-managed, encrypted portal can ensure that all interconnection agreements (voice, SMS, data, IP-peering, Pol, transit, termination, OTT, A2P, content delivery, 5G slicing) are **submitted online** with strict authentication.

This eliminates outdated media such as floppy disks, CDs, DVDs, and even paper copies.

b) Cloud-Native Storage & Versioning

Cloud-native architecture enables:

- Instant retrieval of agreements
- Automated version histories
- Scalable storage
- Encryption-at-rest and encryption-in-transit
- Multi-operator accessibility without duplication

c) Blockchain-Based Audit Trails

Blockchain can provide **tamper-evident logs**, ensuring that:

- Operators cannot retro-modify submitted agreements
- Every amendment is time-stamped and traceable
- Transparency and trust are enhanced

d) AI-Driven Compliance Dashboards

AI analytics can auto-detect:

- Missing clauses
- Deviation from regulations

- Potential anti-competitive patterns
- Delays in submission
- Unusual pricing or discriminatory terms

This creates **proactive compliance** rather than slow, reactive enforcement.

2) Industry Changes

a) End of Legacy Paper/Floppy Workflows

Since 1999, the telecom sector has completely shifted to:

- IP-based interconnection
- Cloud workflows
- E-signature compliance
- Enterprise connectivity
- OTT collaboration

Paper and floppy formats are technologically obsolete and operationally inefficient.

b) Rise of OTT, A2P, ILDO, NLD, and Content Agreements

Agreements today cover:

- OTT partnerships
- A2P SMS & RCS termination
- 5G slices for enterprises
- Content distribution
- International VoIP traffic

These require **rapid updates** that cannot be handled through manual processes.

c) Faster Dispute Resolution

Digital agreements allow:

- Searchable text
- Automatic comparison
- Real-time submission
- Quick retrieval during disputes

This reduces litigation delays and ensures continuity for consumers.

d) Greater Transparency Expectations

Consumers and stakeholders increasingly expect:

- Openness
- Timely disclosure
- Non-discriminatory practices

A digital register aligns with transparency-driven governance.

3) International Practice

a) EU / Ofcom (UK)

- Maintain **fully digital registers** for interconnection and access arrangements
- Allow online public inspection for non-confidential components
- Support secure operator logins for confidential portions

b) FCC (USA)

- Uses **electronic filing systems (ECFS)** for all agreements and regulatory submissions

- Ensures quick public access and searchable formats

c) ITU Guidelines

ITU emphasizes:

- Digitization of regulatory processes
- Transparency
- Online accessibility
- Technology neutrality

India must align with these global norms to support a competitive digital economy.

4) Consumer Benefits

a) Affordability

Better regulatory oversight reduces anti-competitive pricing in interconnection, lowering consumer tariffs for voice, SMS, broadband, and OTT services.

b) Reliability & Service Quality

Transparent agreements and quick dispute resolution ensure:

- Fewer interconnection failures
- Reduced call drops
- Better QoS in IP networks
- Smooth number portability

c) Transparency

Digital registers prevent hidden deals, discriminatory charges, or unfair advantages to dominant operators.

d) Protection from Anti-Competitive Practices

Real-time analytics make it easier for TRAI to detect:

- Predatory pricing
- Discriminatory interconnection
- Blocking or throttling
- Unfair termination charges

This ultimately safeguards consumer interest.

5) Methodology for Implementation

a) Mandatory Online Submission Platform

TRAI should develop a unified digital portal with:

- Secure login for TSPs
- E-signature enabled submission
- Standard templates for agreements

b) Standardized Formats

All agreements should be filed in:

- Machine-readable formats (XML/JSON/PDF-A)
- With mandatory metadata fields (service type, validity, scope, charges, timelines)

c) Regulator-Monitored Dashboards

Dashboards can show:

- Pending/approved agreements
- Amendments
- Date of last update
- Compliance status of each TSP

d) Certified Copies

Nominal online fees can be prescribed for certified copies, ensuring public access without burdens.

e) Timelines

- Submission within **7 days** of signing
- Updates within **48 hours**
- Annual summary certification by TSPs

f) Phased Rollout

1. **Phase 1:** Voluntary upload of new agreements
2. **Phase 2:** Mandatory upload for all new agreements
3. **Phase 3:** Upload of historical agreements
4. **Phase 4:** Sunset clause for physical submissions

g) Multilingual Consumer Communication

Public guidelines should be issued in at least:

- English
- Hindi
- Major Indian languages

This ensures inclusivity and broad consumer awareness.

Conclusion:

Justification Aligned to Global Best Practices and Consumer Protection

The existing provisions under the 1999 Regulations—depending on floppy disks, paper copies, and physical inspections—are incompatible with the modern digital telecom ecosystem. India is now a global leader in digital public infrastructure, 5G rollouts, cloud-native telecom, and massive-scale consumer services.

A secure, digital, transparent, and AI-enabled online Interconnection Register is essential to ensure:

- Non-discriminatory interconnection
- Faster dispute resolution
- Real-time regulatory oversight
- Strong consumer protection
- Global alignment with EU, Ofcom, FCC, and ITU frameworks

Replacing legacy submission systems with an online platform will **strengthen market fairness, enhance transparency, and support affordable, reliable, and high-quality telecom services for all consumers.**

Comparison Table: Current vs Proposed Digital Interconnection Register Framework

Aspect	Current Framework (1999 Regulations)	Proposed Digital Framework (Future-Ready System)
Mode of Submission	Physical submission of agreements in print form , along with floppy disks/CDs containing soft copies.	100% online submission through a secure, regulator-managed digital portal.
Storage System	Manual filing, physical archives, and outdated media (floppy/CD storage).	Cloud-native storage with automated version control, encrypted backups, and searchable metadata.
Access & Inspection	Physical inspection by visiting TRAI office; copies provided manually.	Online inspection through authenticated dashboards, downloadable certified copies.
Transparency Mechanism	Limited visibility; delays in public access; risk of misplaced or outdated files.	Real-time online availability; transparent logs; public access to non-confidential portions .
Technology Architecture	Legacy, non-digital, non-scalable, vulnerable to physical wear and loss.	Secure digital platform with blockchain-based audit trails , e-signatures, and automated timestamps.
Compliance Monitoring	Manual verification of submissions, prone to delays and inconsistencies.	AI-driven compliance dashboards detecting deviations, missing clauses, and discriminatory terms.
Scope of Agreements Covered	Primarily traditional PSTN, TDM voice, SMS, and basic interconnect agreements.	Includes 5G, VoLTE, VoWiFi, IMS/SIP interconnects, OTT partnerships, A2P messaging, IP-peering , and content agreements.
Submission Timelines	Varying timelines, manual delays common.	Mandatory online filing within 7 days , with automated alerts for deadlines.

Aspect	Current Framework (1999 Regulations)	Proposed Digital Framework (Future-Ready System)
Dispute Resolution	Slower due to limited access, manual retrieval, and non-searchable contents.	Faster disputes resolution via searchable text, instant retrieval, and easy cross-comparison.
Security & Integrity	Susceptible to loss, damage, or mistracking of documents.	High security through encryption, traceability, and tamper-evident blockchain records.
Cost Efficiency	Recurrent manual costs for paper, storage, and physical handling.	Lower operational cost with digital efficiency and minimal administrative burden.
Operator Compliance Burden	High — requires physical submissions, couriering, and duplication of documents.	Low — single-window digital filing with standardized templates and automated validation.
Public Transparency	Limited, slow, and dependent on physical availability.	Enhanced transparency through online public inspection portals , aligned with global best practices.
International Alignment	Outdated compared with EU/Ofcom, FCC, ITU digital standards.	Fully aligned with global norms on electronic filing, online registers, digital traceability.
Consumer Impact	Indirect; inefficiencies can lead to higher costs, slower dispute resolution, and inconsistent QoS.	Direct benefits: affordability, reliability, transparency, faster grievance resolution , and protection from anti-competitive practices.
Overall Governance Model	Manual, reactive, fragmented.	Digital, proactive, analytics-driven , and future-ready.

Justification for Replacing the 1999 Interconnection Register Framework with a Modern Digital System

The *Register of Interconnection Agreements Regulations, 1999* was designed for an era of paper-based workflows, PSTN interconnection, and limited digital capabilities. Its reliance on **physical submissions, floppy disks, print copies, and manual inspection** is fundamentally incompatible with today's hyper-digital, cloud-driven, and IP-based telecom ecosystem. A modern, secure, and analytics-enabled online system is essential to ensure regulatory effectiveness, industry efficiency, and robust consumer protection.

First, telecom networks have undergone a complete technological transformation. Interconnection today spans **5G, IMS/SIP, VoLTE/VoWiFi, IP-peering, A2P messaging, OTT collaboration**, and enterprise connectivity. Managing this ecosystem demands **secure digital portals, cloud-native storage, automated versioning, e-signature workflows, and blockchain-based audit trails**. Digital systems ensure tamper-proof logs, automated timestamps, and integrity of submissions—impossible under legacy physical systems.

Second, industry operations have shifted fully to digital workflows. Agreements today evolve rapidly due to dynamic business models, enterprise services, OTT partnerships, and frequent tariff/technology upgrades. The outdated requirements of floppy disks, CDs, and printed copies delay submissions, increase compliance burdens, create inefficiencies, and hinder rapid dispute resolution. A digital portal with **AI-driven compliance dashboards** enables proactive detection of

discriminatory clauses, missing submissions, or deviations from regulatory norms.

Third, international regulatory practice has firmly embraced digital transparency. The **EU/Ofcom, FCC (USA), and ITU** all mandate electronic filing, online registers, and searchable, metadata-rich submissions. India, as a global digital leader, must modernize its interconnection governance framework to align with global standards and ensure predictable, efficient, and transparent regulatory oversight.

Fourth, consumer interest is significantly enhanced through digitalization. Transparent, real-time registers help prevent anti-competitive practices, discriminatory interconnection arrangements, or preferential treatment. Faster dispute resolution leads to improved **service reliability, call completion, number portability, broadband quality**, and lower costs. Digital oversight ensures operators remain accountable, ultimately delivering **affordable, reliable, and high-quality telecom services** to consumers.

Finally, implementation is practical, cost-effective, and future-ready. A phased rollout—starting with voluntary online uploads and moving to full mandatory digital submission—ensures smooth transition. Standardized templates, machine-readable formats, regulator-monitored dashboards, and multilingual public guidance promote compliance and inclusivity. Certified copies can be provided online with nominal charges, eliminating physical handling.

In conclusion, replacing the 1999 physical submission regime with a **secure, online, cloud-native, AI-enabled Interconnection Register** is

imperative for ensuring transparency, strengthening market fairness, reducing compliance burdens, aligning with global best practices, and protecting consumer interests in India's rapidly evolving digital telecom environment.

Q32. Is there a need to incorporate provisions for financial disincentives in interconnection regulations to deter non-compliance? If yes, kindly provide specific scenarios and mention the concerned regulations, where financial disincentives would be applicable, along with their quantification. Kindly justify your response.

Comments :

From a consumer perspective, **interconnection is the invisible backbone** that makes every call, SMS, and digital service work seamlessly across networks. When operators do not comply with interconnection regulations—whether on Quality of Service (QoS), Points of Interconnection (Pols), emergency access, or spam control—the impact is felt directly by consumers as call failures, degraded data quality, spam/fraud, or bill shocks.

In this context, we support the **principle of incorporating financial disincentives** into interconnection regulations, **carefully designed** to be outcome-linked, proportionate, and transparent. These disincentives should not be revenue tools, but **behaviour-shaping mechanisms** that deter non-compliance and promote fair competition, resilience, and consumer protection.

1) Technology Advancement and Need for Enforceable Compliance

SIP/IMS Interconnection and Cloud-Native Pols :

Modern interconnection relies on **SIP/IMS-based IP interconnects, cloud-native Pols, and virtualized network functions**. These technologies make it technically feasible to **monitor traffic in real time**, enforce QoS metrics, and detect congestion, blocking, or discriminatory routing. If such capabilities exist, but operators still choose not to comply, **stronger financial disincentives** are justified.

AI-Driven Observability and Analytics :

With **AI-driven observability**, regulators and operators can track:

- Call completion rates per interconnect
- Dropped calls, failed set-ups, abnormal signaling
- Intentional congestion or throttling at Pols
- Spam and fraud patterns across networks

Because deviations from thresholds can now be **objectively measured**, financial disincentives can be **tied to measurable outcomes** (e.g., persistent call blocking above specified limits).

Caller Authentication and 5G Slicing

Caller authentication (akin to STIR/SHAKEN frameworks) and **5G network slicing** for critical services (health, emergency, enterprise) require **strict interconnection discipline**. If one operator fails to meet prescribed authentication or security standards at interconnect, it can endanger consumers of other networks as well. In such contexts, **non-compliance**

must have clear financial consequences, especially where safety and fraud-prevention are concerned.

2) Industry Changes: From Legacy TDM to IP, with New Risks

Legacy-to-IP Migration and High A2P/Enterprise Volumes

The sector has moved from **TDM/E1-based voice** to **IP, VoLTE/VoWiFi, and high-volume A2P/enterprise messaging**. Misuse of interconnection in this environment (e.g., artificial congestion, discriminatory treatment of OTT or enterprise traffic, blocking of legitimate A2P or critical OTPs) has **direct economic and safety implications** for consumers and businesses.

Spam, Fraud, and Grey-Route Pressures

Spam calls/SMS, spoofed CLIs, and grey routes often exploit **interconnect gaps** between networks. When operators **do not implement mandated spam controls, CLI authentication, or traffic monitoring**, consumers bear the cost in the form of **financial fraud, harassment, and loss of trust**. In such cases, **financial disincentives linked to non-implementation of required safeguards** can drive faster compliance.

Resilience and Redundancy Needs

Modern digital economy services—UPI payments, tele-medicine, online education, emergency alerts—depend on **resilient interconnection with redundancy**. If operators fail to comply with mandated redundancy, emergency interconnect obligations, or minimum PoI capacities, it can lead to **large-scale outages**. Here, **strong disincentives** are essential to ensure operators treat interconnection resilience as non-negotiable.

3) International Practice: Outcome-Linked Remedies and Enforcement

Ofcom/EU Approaches

European frameworks often use **outcome-based remedies** and **significant penalties** when operators breach interconnection duties, QoS obligations, or non-discrimination rules. The emphasis is on:

- Clear obligations
- Evidence-based findings
- Proportionate but strong sanctions

This has helped sustain **effective competition and high consumer trust**.

FCC Enforcement and STIR/SHAKEN-Like Requirements

The FCC in the USA uses **financial penalties, consent decrees, and enforceable commitments** to address non-compliance with interconnection and anti-spam obligations. For caller authentication (STIR/SHAKEN) and robocall mitigation, non-implementation can invite **investigations, penalties, and even call blocking orders**, demonstrating that where consumers are at risk, **mere guidelines are insufficient**.

NG-112 / NG-911 Emergency Frameworks

Next-generation emergency frameworks worldwide (such as NG-112/NG-911) treat **interconnection for emergency calls and location services** as a critical obligation. Non-compliance can trigger **severe regulatory consequences**, recognizing that interconnection failures here can mean **loss of life**. India's own emergency and disaster-management ambitions

similarly justify **strong, enforceable disincentives** for non-compliance with emergency interconnection obligations.

4) Consumer Benefits: Affordability, Reliability, Trust, and Safety

Properly designed financial disincentives **do not hurt consumers**; they **protect** them by shaping operator behaviour:

- **Affordability:** When interconnection is fair and non-discriminatory, it reduces scope for anti-competitive pricing strategies that ultimately raise consumer tariffs. Disincentives for such conduct promote **cost-efficient, competitive markets**.
- **Reliability & QoS:** Penalties for chronic call blocking, congestion, or failure to maintain Pol capacity encourage operators to **invest adequately in interconnection**, improving call completion, QoS, and user experience.
- **Trust & Safety:** Disincentives for failure to implement spam control, caller authentication, and fraud-mitigation reduce **nuisance and financial fraud**, rebuilding consumer trust in telecom services.
- **Emergency Protection:** Strict consequences for non-compliance with emergency interconnection requirements reinforce that **consumer safety is paramount**, ensuring robust availability of emergency services across networks.

5) Proposed Methodology for Incorporating Financial Disincentives

To be effective and fair, financial disincentives must be **clear, proportionate, targeted, and transparent**. A suggested methodology:

(a) Clearly Defined Scenarios

Specify scenarios where financial disincentives may apply, for example:

1. Pol and Capacity Non-Compliance

- Persistent call blocking/congestion above prescribed thresholds due to non-provisioning of mandated Pol capacity.

2. Non-Implementation of Mandated Anti-Spam / Caller

Authentication Measures

- Failure to implement regulator-mandated frameworks for spam control, CLI authentication, or fraud mitigation within stipulated timelines.

3. Discriminatory Interconnection Behavior

- Providing inferior QoS, unreasonable delays, or discriminatory treatment for certain networks or services contrary to regulations.

4. Emergency Interconnection Failures

- Non-compliance with mandated emergency interconnect obligations, redundancy, or routing leading to significant service non-availability.

(b) Linkage to Applicable Regulations

Each disincentive should explicitly reference:

- The **specific regulation, direction, or license condition** that has been breached.
- The **metric** used (e.g., call blocking %, response time, implementation deadline).
- The **observation period** over which non-compliance is measured.

(c) Quantification Bands and Caps

To ensure proportionality and predictability:

- Introduce **bands** (e.g., minor, moderate, severe non-compliance) with **corresponding financial ranges**.
- Consider **per-day or per-week escalation** for continued non-compliance beyond grace periods.
- Provide **overall caps** to prevent excessive punitive impact, while keeping the deterrent meaningful.

Where consumers have directly suffered monetary loss (e.g., fraud reasons attributable to regulatory non-compliance), consider **mechanisms for operator-funded consumer compensation**, subject to clear causality.

(d) Dashboards, Audits, and Observability

Leverage modern technology to ensure that disincentives are based on **verifiable, objective data**:

- Require TSPs to publish **interconnection performance indicators** through **shared dashboards** accessible to TRAI.
- Allow TRAI to use **AI-driven anomaly detection** on SIP/IMS logs and QoS data.
- Introduce **periodic third-party audits** of interconnection compliance and spam/fraud controls.

(e) Phased Rollout and Regulatory Sandboxes

To balance stability with reform:

1. Phase 1 – Voluntary/Advisory Stage

- Publish metrics, start observability, and issue **cautions** rather than penalties.

2. Phase 2 – Limited Binding Disincentives

- Apply financial disincentives to high-risk areas such as emergency interconnection and spam/fraud non-compliance.

3. Phase 3 – Full Implementation

- Extend structured disincentives across all critical interconnection obligations.

Regulatory sandboxes can be used to test **new anti-spam technologies, caller authentication frameworks, 5G slicing interconnect rules**, and associated disincentive structures.

(f) Multilingual Consumer Communication

To maintain public trust and transparency:

- Publish **simplified explanations** in English, Hindi, and major regional languages about:
 - The obligations placed on operators
 - How non-compliance is detected
 - What kind of disincentives can be applied
- Clearly communicate that **the intention is not to increase tariffs**, but to **ensure operators meet their duties** towards consumers.

Conclusion: Prioritizing Consumer Protection and Fair Competition

Given today's **technology capabilities, industry risks, and international experience**, it is both feasible and desirable for interconnection regulations

to incorporate **carefully designed financial disincentives** for non-compliance.

Such disincentives, when **outcome-linked, transparent, and proportionate**, can:

- Deter anti-competitive and discriminatory conduct
- Promote robust interconnection, high QoS, and network resilience
- Accelerate implementation of spam/fraud controls and caller authentication
- Safeguard emergency services and critical digital infrastructure

Above all, they will **prioritize consumer protection and fair competition**, ensuring that India's interconnection regime remains fit for a **5G-ready, AI-enabled, cloud-native, and consumer-centric digital economy**.

Q33. What should be the mechanism and timelines for transition of existing interconnection agreements between the service providers to the new regulatory framework that will emerge from this consultation process? Kindly provide detailed response with justification.

Comments :

India's interconnection ecosystem is undergoing a major transformation as networks evolve to **IP-based, cloud-native, high-volume, AI-observable, and security-sensitive environments**. In this context, transitioning existing interconnection agreements to a new regulatory framework must be **time-bound, minimally disruptive, transparent, and consumer-protective**.

A structured migration plan will ensure continuity of services, prevent disputes, strengthen accountability, and align India with global best practices.

1) Technology Advancement: Why Transition Must Be Structured and Time-Bound

a) SIP/IMS Interconnection and Programmable SBCs

Modern IP/SIP-IMS interconnection allows programmable routing, security policies, QoS enforcement, and real-time analytics. Programmable SBCs and network functions make it technically feasible to **standardize clauses, enforce SLAs, and implement compliance timelines.**

b) Cloud-Native and Virtual Pols

As operators shift to **cloud-native and virtualized Pols**, existing agreements referencing fixed E1/TDM Pols or legacy architecture must be updated. Virtual Pols allow **elastic capacity**, automatic scaling, and redundancy—features that require **updated contractual frameworks.**

c) Verified Calling & Caller Authentication

Caller authentication (akin to STIR/SHAKEN) relies on interconnection agreements that specify:

- Authentication obligations
- Identity header propagation
- Traceback cooperation

Existing agreements must transition to include these **mandatory anti-fraud provisions.**

d) 5G Slicing & QoS Specialization

5G slicing for healthcare, emergency services, industrial automation, and critical IoT introduces **new service classes**, requiring updated:

- QoS definitions
- Routing obligations
- Edge-cloud interconnection terms

Legacy agreements cannot support these advanced requirements.

e) AI-Driven Observability & Compliance

AI-based interconnect monitoring enables **automated detection of congestion, blocking, anomalies, grey-route behaviour, and spam**. Agreements must incorporate obligations for **data-sharing, telemetry, and real-time auditability**, necessitating standardized updates.

2) Industry Changes: Why Legacy Agreements Cannot Continue Unmodified

a) Migration from TDM/E1 to IP/IMS

Existing agreements reference:

- TDM trunks
- E1 capacity
- Legacy metrics

These are incompatible with **IP-based bandwidth, packets, sessions, CPS, and latency/jitter/loss metrics** used today.

b) OTT, A2P, and Enterprise Growth

OTT interconnects, A2P SMS, RCS, enterprise APIs, and cloud platforms require modern revenue-sharing, SLA, routing, and anti-fraud clauses—absent in most legacy agreements.

c) Grey-Route and Fraud Pressures

Outdated agreements lack:

- Verified CLI obligations
- Header integrity rules
- Spam/smishing controls
- Traceback responsibilities

Transition timelines must ensure **rapid inclusion of these safeguards**.

d) Resilience and Security Needs

UPI, telemedicine, online education, disaster alerts, and digital governance depend on **resilient and secure interconnection**. Legacy agreements do not adequately cover redundancy, security coordination, or cyber-resilience.

3) International Practice Supporting Phased Transition

a) EU/Ofcom Phased Market Reviews

EU and Ofcom transition regimes follow:

- **Defined phases** for migrating agreements
- **Clause templates** for harmonization

- **Outcome-linked compliance monitoring**

India can adopt a similar phased migration with strict time limits.

b) FCC Electronic Filing & Transition Orders

The FCC routinely issues:

- Transition orders for interconnection reforms
- Mandatory digital filing requirements
- Sunset dates for outdated practices

This ensures clarity and avoids prolonged dual frameworks.

c) ETSI/3GPP Interoperability Baselines

ETSI/3GPP technical baselines (IMS, SIP, VoLTE, emergency calling, authentication) require contractual alignment. Agreements must be updated to reflect these **global technical norms**.

d) NG-112/NG-911 Emergency Frameworks

Next-generation emergency frameworks require:

- Caller identity verification
- Real-time location
- Redundant routing

Legacy agreements do not address these obligations; timely transition is essential for **public safety**.

4) Consumer Benefits from a Timely and Orderly Transition

a) Affordability

Harmonized and modern agreements reduce operational inefficiencies and disputes, lowering backend costs and supporting **affordable tariffs**.

b) Reliability

Updated QoS clauses, redundant routing, and virtual Pols ensure **better call completion, fewer outages, and smoother emergency services**.

c) Trust

Verified calling, anti-fraud obligations, and analytics-backed monitoring reduce spam, spoofing, and fraud, enhancing **consumer trust**.

d) Safety

Emergency calling improvements, 5G slicing integrity, and inter-operator security coordination directly improve **public safety and emergency responsiveness**.

e) Transparency

Clear migration timelines and digital filing make the system predictable and transparent for all stakeholders.

5) Methodology for Implementation: A Phased, High-Certainty Transition Plan

A **five-pillar** methodology is suggested to make the transition predictable and minimally disruptive.

Pillar 1: Phased Transition Plan with Clear Milestones

Phase 0: Pre-Transition (0–30 days)

- Publish new interconnection framework.
- Provide templates and metadata requirements.
- Begin operator training and sandbox testing.

Phase 1: Mandatory Mapping (30–90 days)

Operators map all existing agreements to:

- New regulatory clauses
- Technical obligations
- Security/QoS standards
- Telemetry and data-sharing needs

A standardized **mapping template** should be provided by TRAI.

Phase 2: RIO Updates & Alignment (90–150 days)

- All operators publish revised RIOs aligned to the new framework.
- TRAI reviews and approves within defined timelines.

Phase 3: Agreement Transition (150–270 days)

- All bilateral/multilateral agreements must be renegotiated or updated.
- Operators must file digital copies on TRAI's portal.
- All agreements must incorporate new obligations for:
 - SIP/IMS
 - 5G slicing
 - Verified calling
 - Virtual Pols
 - AI-driven observability

- Anti-spam/fraud controls

Phase 4: Sunset of Legacy Agreements (270–360 days)

- All legacy clauses referencing E1/TDM or outdated security/QoS metrics become invalid.
- Universal shift to the new framework.

Pillar 2: Clause Mapping & Change Control

- TRAI should mandate a **clause-by-clause mapping exercise** for each existing agreement.
- Material deviations must be flagged and justified.
- Change control logs must be attached to each amendment.

Pillar 3: Data-Backed Audits and Observability

- Require operators to share SIP/IMS signaling KPIs, Pol metrics, congestion logs, and anti-spam performance.
- TRAI should use **AI-based anomaly detection** to verify compliance.
- Independent audits on emergency routing, redundancy, and verified calling.

Pillar 4: Dashboards & Dispute Resolution Mechanism

- TRAI should publish:
 - Transition status dashboards
 - RIO revision status
 - Agreement filing status
 - Compliance alerts

- A **fast-track dispute resolution mechanism** is required for transition-related disagreements.

Pillar 5: Multilingual Consumer & Stakeholder Communication

Clear public explanations in:

- English
- Hindi
- Regional languages

should cover:

- Purpose of transition
- Expected improvements
- Impact on emergency services
- Consumer safety measures

This enhances transparency and builds trust.

Conclusion: A Time-Bound, Minimally Disruptive, Globally Aligned Transition

A transparent, structured transition of existing interconnection agreements is essential to support India's move toward **cloud-native interconnection, IP-SIP frameworks, 5G slicing, verified calling, and AI-driven compliance.**

A phased, time-bound plan—supported by templates, dashboards, clause-mapping, RIO updates, and audits—ensures **minimal service disruption,**

protects consumers, and aligns India with **EU/Ofcom, FCC, ETSI/3GPP, and NG-112/NG-911 global best practices.**

Such a transition will reinforce:

- **consumer affordability,**
- **network reliability,**
- **public safety,**
- **spam/fraud protection, and**
- **industry-wide transparency.**

This is fundamental to building a **trusted, resilient, and future-ready digital communications ecosystem** for India.

Comparison Table: Current vs Proposed Transition Mechanism for Interconnection Agreements

Aspect	Current Mechanism (Status Quo)	Proposed Future-Ready Transition Mechanism
Regulatory Basis	No unified transition framework; operators rely on bilateral negotiations and legacy circulars.	A single national transition framework , clearly aligned to new interconnection rules emerging from this consultation.
Technology Alignment	Agreements reflect legacy TDM/E1, PSTN, SS7 , with partial IP/SIP clauses retrofitted.	Agreements fully aligned to SIP/IMS, cloud-native/virtual Pols, programmable SBCs, verified calling, 5G slicing, AI observability.

Aspect	Current Mechanism (Status Quo)	Proposed Future-Ready Transition Mechanism
Mapping of Existing Agreements	No mandated mapping or template; operators interpret changes independently.	Mandatory clause-mapping exercise using TRAI-prescribed templates for all existing agreements.
RIO (Reference Interconnect Offer) Updates	RIOs updated infrequently, often after delays; no defined review cycle.	Time-bound RIO revision within 90–150 days, aligned to new rules, with regulator approval timelines.
Transition Timelines	Undefined, operator-driven, often leading to multi-year coexistence of outdated and updated terms.	Phased, time-bound transition with sunset dates (e.g., 12 months), minimizing dual-framework overlap.
Dispute Resolution	Mostly bilateral negotiation; disputes escalate slowly through standard regulatory processes.	Fast-track, transition-specific dispute resolution , focusing on clause alignment, PoI obligations, security, and QoS.
Technology Migration Support	Limited guidance for TDM→IP migration; operators choose their own approach.	Structured migration support for SIP/IMS, virtual Pols, telemetry, verified calling, spam control, and 5G slicing obligations.
Emergency Services Integration	Legacy routing rules; limited accountability for NG-112/NG-911 equivalent features.	Agreements updated to comply with next-generation emergency frameworks , redundancy, verified identity propagation, and location standards.
Security & Anti-Fraud Clauses	Often outdated; missing verified calling, header	Mandatory inclusion of: verified calling/STIR-SHAKEN-like

Aspect	Current Mechanism (Status Quo)	Proposed Future-Ready Transition Mechanism
	integrity, traceback cooperation, and spam control obligations.	requirements, anti-spoofing rules, spam/fraud mitigation, and traceback processes.
Grey-Route & A2P Controls	Weak controls due to outdated definitions and unilateral interpretations.	Clear, enforceable A2P/OTT/enterprise traffic definitions , grey-route prevention rules, and telemetry-backed monitoring.
Monitoring & Observability	Primarily manual or bilateral; limited visibility of real-time SIP/IMS performance or Pol congestion.	AI-driven observability dashboards , SIP logs, Pol congestion KPIs, anomaly detection, and regulator visibility.
Audit Requirements	No uniform audit framework; audits vary across operators.	Mandatory periodic audits of interconnection KPIs, emergency routing, verified calling, and security implementation.
Filing & Documentation	Filing depends on physical submission or PDFs; non-standard formats.	100% electronic filing with metadata, searchable formats, version control, and online public inspection of non-confidential sections.
Change Control Process	Unstructured amendments over time, resulting in inconsistent agreements.	Standardized change control , unified templates, and operator-level change logs submitted to TRAI.
Consumer Transparency	Indirect consumer impact; limited transparency on interconnection changes.	Public dashboards showing transition status, improved safety

Aspect	Current Mechanism (Status Quo)	Proposed Future-Ready Transition Mechanism
		measures, and QoS gains— enhancing consumer trust.
Impact on Competition	Uneven adoption of new terms can create competitive advantage for certain operators.	Simultaneous, phased adoption ensures a level playing field and fair competition.
Overall Consumer Experience	Risk of call failures, spam, inconsistent QoS, limited emergency reliability.	Improved affordability, reliability, fraud protection, verified calling, emergency readiness, and transparency.

Justification for the Proposed Transition Mechanism

The transition from legacy interconnection agreements to a modern, technology-aligned regulatory framework is essential for ensuring fair competition, seamless interoperability, and consumer protection in India’s rapidly evolving digital communications ecosystem. The comparison table highlights key gaps in the current transition environment and demonstrates why a **structured, time-bound, and technology-driven transition mechanism** is critical.

First, existing agreements were drafted for a different technological era—dominated by **TDM/E1, PSTN, SS7 signalling**, and limited digital services. Today’s networks operate on **SIP/IMS architectures, cloud-native and virtual Pols, programmable SBCs, verified calling, 5G slicing, and AI-driven observability**. Legacy agreements cannot support emerging

requirements such as caller authentication, emergency service modernization, enterprise traffic management, and advanced QoS metrics.

Second, industry developments—growth in **OTT services, A2P messaging, enterprise connectivity**, and rising **spam/fraud and grey-route pressures**—demand interconnection agreements with clear security, anti-spoofing, telemetry, traceback, and redundancy obligations. Many current agreements do not incorporate these safeguards, exposing consumers to avoidable risks.

Third, international experience consistently supports phased, regulator-led transitions. The **EU/Ofcom** rely on structured market reviews and sunset timelines; the **FCC** mandates digital filing, transition orders, and unified templates; **ETSI/3GPP baselines** ensure technical interoperability; and **NG-112/NG-911 frameworks** mandate time-critical emergency interconnection obligations. India must adopt similar approaches to harmonize agreements and provide legal certainty.

Fourth, consumers directly benefit from a smooth transition. Updated agreements enhance **affordability** through lower backend costs, improve **reliability** via modern QoS and redundancy frameworks, increase **trust** through verified calling and anti-spam obligations, and strengthen **safety** via robust emergency routing, identity propagation, and location accuracy.

Fifth, the proposed mechanism incorporates a **phased transition plan**, including clause mapping, standardized RIO updates, online filing, observability dashboards, data-backed audits, and fast-track dispute resolution. These tools ensure a predictable transition that avoids service

disruption, minimizes inter-operator disputes, and supports time-bound adoption of new standards.

In summary, migrating existing agreements to the new regulatory framework through a structured, milestone-based process is essential for maintaining continuity, protecting consumers, ensuring network resilience, and aligning India with global best practices. A defined transition mechanism provides clarity, transparency, and accountability—delivering a telecom ecosystem that is **future-ready, secure, and consumer-centric**.

Q34. What should be the interconnection framework for satellite-based telecommunications networks with other telecom networks? Further, whether the interconnection frameworks for MSS and FSS satellite-based telecommunications networks should be distinct? Please provide your response along with end-to-end diagrammatic representation and justification in respect of the following: a. Satellite - Satellite network interconnection b. Satellite - PLMN interconnection c. Satellite - PSTN interconnection.

Comments :

1) Technology advancement and implications for interconnection

a) LEO/MEO/GEO architectures

- **LEO** constellations (hundreds to thousands of satellites at ~500–1400 km) offer low latency (20–40 ms one-way) and global coverage with frequent handovers and moving beams.

- **MEO** constellations (~8000–12000 km) balance coverage and latency.
- **GEO** satellites (~35,786 km) provide wide coverage and stable beams but with high latency (~250 ms one-way).

3GPP Release-17 and onwards explicitly standardise **Non-Terrestrial Networks (NTN)** so that 5G NR and NB-IoT can operate over LEO/GEO systems with appropriate timing and Doppler compensation.

Interconnection implications:

- Interconnection frameworks must **not hard-code latency and jitter assumptions** based on terrestrial links only.
- QoS, charging and SLAs must allow **different latency envelopes and jitter bounds** for GEO vs LEO/MEO paths.
- Routing and policy control (PCC/PCF) need latency-aware treatment so that critical services (emergency, financial transactions, real-time control) are preferentially routed via LEO/MEO or terrestrial where possible.

b) Bent-pipe vs regenerative payloads

- **Bent-pipe (transparent) payloads** act like RF repeaters: baseband processing and IP/SIP interworking happen at the gateway on the ground.
- **Regenerative payloads** perform on-board processing, routing and sometimes 5G gNB-DU/gNB-CU or IP/MPLS functions in space.

ETSI SES specifications already address IP interfaces at satellite terminals and gateways, treating them as IP network elements.

Interconnection implications:

- For **bent-pipe systems**, the main interconnect point is a **satellite earth station gateway (SESG)** or hub that terminates satellite waveforms and presents **IP/SIP, Diameter/HTTP2 (5G SBA)** interfaces to PLMN/NGN networks.
- For **regenerative systems**, the interconnection may effectively occur at **on-board “edge routers” or gNBs**, but from the national perspective it should still be abstracted as a **logical gateway** with well-defined IP/SIP interconnect points.
- Regulations should be **agnostic to payload type**, but must insist that **all interconnection for public services happens at licenced, auditable logical gateways** where lawful intercept, security, and QoS enforcement are possible.

c) 5G NTN integration, SIP/IMS over satellite, and beam handover

3GPP NTN work (Release-17 and evolving Release-18/Release-19) defines how 5G NR and NB-IoT operate via satellites, including **Doppler, timing advance, random access, beam management and mobility procedures**. GSMA NTN guidance emphasises hybrid cellular/satellite offerings, roaming integration and direct-to-device (D2D) NTN.

Interconnection implications:

- **SIP/IMS over satellite** must support:
 - Enhanced jitter buffers and echo control.
 - Session continuity during **beam handover / satellite handover**.

- Interworking with **VoLTE/VoNR** and legacy CS voice via standard interconnect trunks (SIP-I, SIP-T, or ISUP).
- Interconnection rules should **mandate IPv6 and SIP/IMS-ready interconnect at satellite gateways**, ensuring that NTN subscribers can roam and interwork with terrestrial PLMNs as ordinary 4G/5G users.
- Handover between satellite and terrestrial access (e.g., device moves from satellite coverage to terrestrial macro cell) requires **common subscriber profiles and policy control** in the core network; interconnection must not create artificial barriers to such multi-access functionality.

d) QoS, security, and edge gateways

Keysight, GSMA and others highlight that NTNs must support **end-to-end QoS, timing accuracy, and security** comparable to terrestrial systems for many use-cases.

Interconnection implications:

- **Satellite gateways and edge POPs** should be treated as **strategic interconnection points**, with:
 - End-to-end QoS classification (e.g., conversational voice, critical IoT, best-effort data).
 - IPsec/DTLS or equivalent encryption between satellite terminals and gateways, with **trusted IP domains** between gateways and PLMN/NGN cores.
 - Hooks for **STIR/SHAKEN-like caller authentication**, anti-fraud analytics, and DDoS/signal manipulation protection.

2) Industry changes and use-cases

a) Emerging LEO constellations and enterprise backhaul

New LEO constellations and “Satellite 2.0” direct-to-device services are moving from backhaul-only to **consumer-facing and IoT-facing services**, with 3GPP-compliant NTN access.

For enterprises, satellites are already used for:

- **Rural and remote backhaul** for mobile operators.
- **Cloud on-ramps** and connectivity for offshore rigs, mines, railways and remote campuses.
- **Quick-deploy connectivity** for events and field operations.

Interconnection implications:

- Regulatory frameworks should allow **flexible IP interconnect** where satellite operators can offer:
 - wholesale backhaul to PLMNs,
 - IPVPN/MPLS to enterprises, and
 - direct access services (MSS-type) to end users.
- Interconnection charges and QoS obligations must reflect **shared or sliced backhaul** used by multiple services.

b) Disaster recovery and public safety

Satellites are uniquely suited for **disaster recovery, emergency communications and early-warning dissemination**, when terrestrial infrastructure is damaged. GSMA and 3GPP NTN work highlight emergency scenarios as a key NTN case.

Interconnection implications:

- Interconnection rules should:
 - Prioritise satellite traffic for **emergency numbers and public-warning systems**.
 - Ensure **free-to-caller or capped emergency roaming** across satellite and terrestrial networks.
 - Preserve **location information and call routing integrity** even over satellite paths (using hybrid GNSS + network-based methods).

c) IoT, maritime, aviation and spectrum sharing

ITU-R and NFAP-style national plans explicitly differentiate spectrum allocations for **MSS, FSS and BSS**, and study sharing and interference between them.

Key industry changes:

- Massive IoT via NTN (agriculture, logistics, environmental monitoring).
- High-throughput connections for **ships, aircraft, and unmanned platforms**.
- More dynamic **spectrum sharing** between MSS and FSS, and with terrestrial services.

Interconnection implications:

- IoT services need **lightweight signalling, efficient small-payload handling, and event-driven charging** at interconnect points.

- Aviation and maritime safety services require **high availability and integrity**, implying **tighter QoS and security obligations** at satellite interconnects.
- MSS and FSS frameworks must be distinct enough to handle **mobility vs fixed earth stations**, but harmonised at the IP layer so that **applications and consumers see consistent behaviour**.

3) International practice: standards and regulatory norms

a) 3GPP NTN specifications

3GPP has standardised NTN support in **Release-17** and is enhancing it in **Release-18+**, covering:

- 5G NR NTN and NB-IoT NTN.
- Satellite-specific PHY/MAC adaptations, random access and mobility.
- Integration with existing 5G core (5GC) for roaming and interworking.

Regulators can leverage these specifications to define **minimum technical baselines** for interconnection (supported codecs, QoS classes, signalling protocols, etc.).

b) ETSI and ITU-R recommendations

- ETSI SES standards define **Earth stations, IP interfaces, control-plane and user-plane specs** for MSS/FSS systems, including harmonised ENs for user equipment and gateways.
- ITU-R S-Series (FSS) and M-Series (MSS) recommendations address **frequency allocation, interference, coordination, and sharing**

between FSS, MSS and other services, including statistical methods for interference evaluation.

These support a **clear distinction** between MSS and FSS in spectrum and coordination terms, while encouraging **coexistence and sharing**.

c) GSMA guidelines, emergency and lawful intercept norms

- GSMA NTN and IoT reports stress the need to integrate NTNs into **existing roaming, numbering, and emergency call frameworks**, and to ensure **sim-based identity and standardised APIs**.
- Lawful interception (LI) and data-retention rules in ITU-T/ETSI are generally applied at **network gateways and core network elements**, which aligns with the proposed **gateway-centric interconnection model**.

Regulatory takeaway: global practice is converging on **IP/SIP-centric, gateway-based interconnection** for satellite networks, with MSS/FSS distinctions at radio and service layers rather than at the core interconnect layer.

4) Consumer benefits: coverage, reliability, safety, affordability, resilience

A well-designed interconnection framework directly benefits consumers:

1. Coverage & inclusion

- Satellites complement terrestrial networks, bringing connectivity to **remote, rural, maritime, and underserved areas**.

- Interconnection ensures that users on satellite links can **call, message, and access services on any other network as seamlessly as urban mobile users.**

2. Reliability & resilience

- During disasters or terrestrial outages, satellites provide **backup routes**. Proper interconnection ensures **automatic failover** so that calls to emergency numbers and essential services complete reliably.

3. Safety & security

- Standardised interconnects with strong authentication and LI enable **traceable, accountable communications**, reducing fraud, spoofing and misuse.
- For aviation and maritime sectors, interoperable satellite links enhance **situational awareness and distress communication.**

4. Affordability & transparency

- Harmonised interconnection and competition between providers can reduce **monopoly rents for satellite backhaul or roaming**, lowering user tariffs over time.
- Clear rules on **tariff disclosure, bill shocks and fair-use policies** across satellite and terrestrial networks protect consumers.

5. Innovation & choice

- A common interconnect framework enables innovative services (hybrid satellite-cellular plans, global IoT, remote tele-education and tele-medicine) while giving consumers the

freedom to choose providers and devices without being locked into proprietary silos.

5) Proposed methodology for implementation

a) Distinct MSS/FSS profiles with harmonised IP/SIP layer

1. Separate MSS vs FSS regulatory profiles

- **MSS profile:**
 - Focus on **mobile terminals, direct-to-device, maritime/aviation/mobility services.**
 - Strong obligations on **emergency calling, roaming, and QoS for conversational services.**
 - Tight integration with PLMNs and numbering plans.
- **FSS profile:**
 - Focus on **fixed earth stations, gateways, enterprise backhaul and broadcast-style services.**
 - Emphasis on **capacity, quality of backhaul, resilience, and interference management.**
 - Interconnection mainly at **IP/MPLS and SIP trunks** between satellite gateways and PLMN/NGN cores or enterprise networks.

2. Harmonised interconnection at the IP/SIP layer

- Require both MSS and FSS licensees to expose **standardised interconnect reference points:**
 - IP (IPv4/IPv6) with support for IPsec and QoS markings (DiffServ).
 - SIP/IMS trunks for voice and messaging.

- REST/JSON and standard APIs for IoT and network control (resource ordering, QoS APIs, coverage maps).

b) IP/SIP interconnect at gateways and QoS classes

- Mandate **gateway-centric interconnection**, where each licenced satellite network (MSS or FSS) has one or more **SESGs / POPs** that:
 - Peer with PLMN cores (S8/N6/NG, IMS, SBCs) and IP networks.
 - Support **multi-class QoS**, at least:
 - QCI/5QI-type bearer classes for conversational voice and video.
 - Classes for **critical IoT / emergency alerts**.
 - Best-effort data.
- Define **interconnect SLAs** per class (latency bands for LEO vs GEO, availability, packet loss, jitter) and require **reporting via regulator dashboards**.

c) Authenticated routing and standard APIs

- Enforce **strong identity and authentication** at interconnect points:
 - SIM-based / eSIM identities for NTN devices.
 - Support for **caller ID authentication frameworks** (e.g., STIR/SHAKEN-like) and robust anti-fraud analytics.
- Provide **standardised APIs** for:
 - Coverage and beam-footprint information.
 - Network status and planned outages.
 - Emergency priority activation and disaster “fast-track” provisioning.

d) Dashboards, monitoring and transparency

- Require satellite and terrestrial interconnect partners to publish **regulator-facing dashboards** with:
 - KPIs per QoS class.
 - Congestion and outage reports.
 - Emergency call success ratios and time-to-connect statistics.
- Regulators can use this to:
 - Detect **discriminatory treatment** of satellite traffic.
 - Enforce **non-discriminatory routing and fair access**.

e) Phased rollout and multilingual consumer communication

- Adopt a **phased implementation**:
 1. **Phase 1** – basic IP/SIP interconnect, emergency call support, minimal QoS reporting.
 2. **Phase 2** – full 5G NTN integration, roaming, QoS-differentiated charging, regulator dashboards.
 3. **Phase 3** – advanced APIs, dynamic slicing for critical IoT/public safety, cross-border harmonisation.
- Accompany each phase with **multilingual consumer communication**:
 - Clear explanation of coverage, tariffs, QoS expectations for satellite-backed services.
 - Explicit disclosure of **latency, possible service limitations, and fair-use policies**.

6) Should MSS and FSS frameworks be distinct?

Yes – MSS and FSS frameworks should be distinct at the radio/service level but harmonised at the interconnection (IP/SIP) layer.

- MSS deals with **mobile, direct-to-terminal services**, requiring:
 - Stronger focus on **emergency calling, QoS for conversational services, roaming, consumer-grade tariffs and retail protections.**
 - Device, SIM/eSIM, and handset-centric regulation.
- FSS deals with **fixed earth stations, gateways and wholesale/enterprise services**, requiring:
 - Emphasis on **capacity, interference management, gateway licensing, and wholesale SLAs.**
 - Enterprise and operator-centric regulation for backhaul and cloud access.

If both were forced into a single, undifferentiated framework:

- Consumers might either **lose protections** in MSS scenarios or **face unnecessary retail-style constraints** in enterprise FSS scenarios.
- Regulators would struggle to tailor **spectrum, licensing, and QoS obligations** to very different use-cases.

A **layered approach**—distinct MSS/FSS profiles but a **common, IP/SIP-based interconnection framework and common consumer-protection principles**—captures the best of both worlds.

7) Conclusion and justification aligned to global best practices

Globally, standards and emerging commercial deployments are converging on a model where satellites are treated as **standard network access technologies integrated into 4G/5G and IP ecosystems**, supported by:

- 3GPP NTN specifications for **radio and core network integration**.
- ETSI and ITU-R frameworks differentiating **MSS and FSS** in spectrum and coordination terms while enabling shared use and coexistence.
- GSMA guidance emphasising **hybrid cellular–satellite offerings, roaming, and direct-to-device models** anchored in standard IP/SIP and SIM-based identity.

A **consumer-centric interconnection framework** that:

- recognises **MSS and FSS as distinct service families**,
- mandates **gateway-based IP/SIP interconnection** aligned with 3GPP/ETSI standards,
- enforces **QoS, security, emergency and LI obligations**, and
- ensures **affordable, transparent tariffs and multilingual communication**

will:

- extend **coverage and inclusion**,
- enhance **safety, reliability and resilience**,
- foster **innovation and competition**, and
- remain aligned with **global best practices and evolving NTN/6G standards**.

Such a framework ensures that the benefits of the satellite revolution reach **all consumers – urban and rural, on land, at sea, and in the air – with trust, transparency and protection at its core.**

Q35. Are there any specific regulatory models from other countries that have successfully addressed interconnection related issues and challenges which can be adapted in the Indian telecom sector? If yes, kindly provide details of such international best practices.

Comments :

1. Technology advancement

How regulators have used IP, IMS/SIP, ENUM, IPv6 & QoS to modernise interconnection

(a) EU

- **Shift from TDM/SS7 to SIP/IMS in NGN frameworks**

European regulators (through the EU framework and CEPT/BEREC work) explicitly recognise that IP-based interconnection is the end-state, with **SIP replacing SS7 signalling at interconnection points** while retaining the same conceptual P2P interconnect model. Many NRAs allow/encourage operators to agree IP interconnect commercially, while using legacy fixed/mobile termination remedies only as a safety net.

- **NGN & QoS classes**

EU member states regulate QoS via the EECC and national rules, using ITU-T/ETSI guidance for parameters like latency, jitter and packet loss in NGN. DiffServ-style QoS classes (EF, AF, BE) are used

in IP interconnect offers, even if enforced “light-touch” rather than per-packet policing by regulators.

- **IPv6 and resilience**

The EU promotes IPv6 as foundational for a resilient, scalable NGN, linking IPv6 deployment to the Digital Single Market and public-sector digitisation. This dovetails with interconnection: regulators expect new NGN/IMS interconnect platforms to be IPv6-ready by default.

(b) United States (FCC)

- **IP interconnection and VoIP**

The FCC recognises VoIP/IP interconnection as critical to the IP transition, highlighting that **non-IP segments in a call path break caller ID authentication (STIR/SHAKEN)** and degrade reliability.

The policy direction: encourage IP-to-IP interconnection between carriers, sunset mandatory TDM POIs over time, and align interconnection with anti-robocall frameworks.

- **Security & resilience baked into interconnection**

Caller ID authentication and robocall mitigation are deeply tied to SIP signalling at interconnects; the FCC uses this to justify accelerating the IP transition as a resilience and trust measure.

(c) Singapore (IMDA)

Singapore is probably the **cleanest template** for India:

- **Dedicated IP-based interconnection regime**

IMDA ran a multi-year process on IP interconnection and then issued a formal **decision to implement IP-based interconnection**, including:

- Transition timetable from TDM to IP,
- Finalisation of SIP standards/specifications via a technical task force,
- Alignment of **fixed number portability** mechanisms with IP interconnect, and
- Rules for RIOs in an IP environment.

- **IP RIOs for dominant operators**

In 2025, IMDA approved a new **Singtel RIO specifically for IP-based voice interconnection**, including technical, QoS and operational terms.

- **ENUM & portability**

The IP-based regime integrates portability using database-based routing (ENUM-like mechanisms) so that number portability and routing work consistently across IP interconnects.

(d) Australia (ACCC)

- **IP-aware treatment of mobile termination**

ACCC's declaration of the **Mobile Terminating Access Service (MTAS)** explicitly defines termination from a "point of interconnection to the B-party on a digital mobile network", a technology-neutral description that fits TDM or IP.

In 2024 it extended MTAS declaration to 2029, maintaining cost-oriented regulation while networks transition to all-IP.

- **Ongoing work on IP voice interconnection**

ACCC consults on non-price terms and conditions for voice interconnection services, including IP-based POIs and QoS obligations.

(e) South Korea (KCC)

- **NGN backbone and converged IP “BcN”**

Korea’s “Broadband Convergence Network (BcN)” vision (captured in ITU case studies) describes an integrated IP infrastructure for wired/wireless, supporting QoS and multiple services on a single NGN.

- **Interconnection & network-usage rules for CPs**

Recent changes to the Telecommunications Business Act impose **interconnection-style obligations (network usage fees + QoS requirements) on large content providers**, effectively extending IP interconnection issues to the CDN/OTT layer.

(f) Japan (MIC)

- **NGN competition rules & IP transition**

Japan’s MIC set up a **Study Group on competition rules for IP-based networks**, examining how interconnection and competition law must change as NGN/IMS becomes dominant.

- **Number portability and IP routing**

Japanese operators developed domestic **number portability**

specifications that rely on central databases and IP routing, paving the way for ENUM-like solutions in NGN.

- **Regulatory base: Telecommunications Business Act**

The Act sets the core rules on connection between carriers, charges and universal service, and is progressively updated to reflect 5G/NGN realities.

Takeaways for India under this pillar

- Treat **IP-based interconnection, IMS/SIP, ENUM and IPv6** as *regulatory primitives*: specify them in codes, RIO templates and technical standards.
- Use **QoS classes** (DiffServ-style) with measurable parameters (packet loss, jitter, latency), but keep enforcement outcome-based rather than micromanaging internal design.
- Hard-link **security & resilience** (STIR/SHAKEN-like frameworks, emergency call integrity) to IP interconnection obligations, as the FCC is doing.

2. Industry changes

Structural reforms, cost orientation, RIOs, and dispute resolution

(a) Cost-oriented termination & bill-and-keep

- **EU**: NRAs have long mandated **cost-oriented fixed and mobile termination rates for SMP operators**, using bottom-up LRIC models and gradually reducing asymmetry to move closer to “near bill-and-keep” for many intra-EU situations.

- **US:** The FCC's intercarrier-compensation reforms pushed **domestic voice termination toward bill-and-keep**, reducing arbitrage and encouraging flat-rate, all-distance offers to consumers.
- **Australia:** ACCC keeps **regulated MTAS** as a declared service, periodically reviewing pricing approaches to reflect cost and technological change while remaining technology-neutral.
- **South Korea:** KCC directly sets cost-based interconnection prices, considering supply costs, reasonable profit and impact on competition.

(b) Functional separation and open access

- **EU & some OECD countries** use functional separation/strong equivalence of input (EoI) obligations on incumbents' wholesale arms to ensure **non-discriminatory interconnection**, especially where they control key NGN infrastructure.
- **Japan & Korea** rely more on competition law + non-discrimination obligations and ex-ante SMP regulation, but still require transparent, published interconnect terms.

(c) Standardised RIOs & interconnect offers

- **Singapore:** IMDA mandates **Reference Interconnection Offers** from dominant operators; these RIOs must cover technical specs, QoS, operational processes and charges, and are subject to public consultation and approval.
- **EU:** Many NRAs require SMP operators to publish reference offers (for interconnect, bitstream, access, etc.), often reviewed by the regulator/bodies like BEREC.

- **Australia:** While there isn't a single "RIO" label, ACCC's access determinations serve a similar function, providing standard terms and conditions for declared services.

(d) Dispute resolution mechanisms

- **IMDA:** Encourages commercial negotiation but keeps a **formal dispute-resolution power** if parties cannot agree, with structured timelines and clear evidentiary requirements.
- **ACCC:** Undertakes public inquiries and can impose binding access determinations when commercial negotiations fail, ensuring essential wholesale services remain accessible.
- **KCC & MIC:** Have statutory powers to intervene in interconnection disputes, approve tariffs and, if necessary, mandate changes to promote fair competition.

India lens for this pillar

- India already uses **cost-oriented IUC and RIO-style reference interconnect offers**. The next step is to:
 - Re-cast these into an **IP-native framework** (SIP/IMS, QoS classes),
 - Decide where **bill-and-keep** is appropriate (e.g., domestic on-net/off-net voice, some IP peering) vs. where cost-based charges are still necessary (e.g., satellite/NTN, rural access).

3. Consumer benefits

How these models improved affordability, reliability, portability, security & QoS

Across jurisdictions, a few clear consumer outcomes keep repeating:

1. **Affordability & tariff simplification**

- Cost-oriented or bill-and-keep termination removes extreme off-net/on-net differentials and long-distance surcharges; this is visible in the EU's move to low, symmetric termination rates and the US bill-and-keep model, which support flat-rate nationwide calling.
- ACCC's MTAS regulation explicitly aims to keep retail prices for off-net mobile calls reasonable.

2. **Reliability and resilience**

- Coherent IP interconnection (end-to-end SIP/IMS) reduces failure points and improves HD-voice consistency; even industry analyses in the US emphasise fewer failed call hand-offs and easier troubleshooting in an all-IP interconnect environment.
- EU/ITU guidance on QoS regulation encourages published, monitored QoS indicators, which give consumers stable expectations and strengthen accountability.

3. **Portability and “any-to-any” connectivity**

- IP-based number portability (ENUM-style databases) used in Japan and integrated into Singapore's IP interconnection decision ensure that **changing operators does not break reachability**, reducing lock-in and encouraging competition on quality and price.

4. **Security and trust**

- The FCC's linkage of IP interconnection to **STIR/SHAKEN caller ID authentication** directly addresses fraud and

unwanted calls; a fragmented TDM/IP interconnect landscape makes it easier for bad actors to spoof identity.

- South Korea's rules imposing QoS and network-usage requirements on large CPs aim to ensure that high volumes of traffic (e.g., video, gaming) don't degrade overall user experience.

5. Service quality for advanced apps

- NGN frameworks (EU, Japan, Korea, Australia) explicitly use QoS classes and traffic management to support **real-time applications** (VoIP, video, telemedicine), with regulators slowly moving from best-effort to measurable, class-based QoS targets. For India, these translate into:
 - Stable, low, and predictable **on-net/off-net tariffs** and future-proof treatment of 5G/VoWiFi/IMS voice.
 - More reliable **emergency calling, HD voice and video**, especially across TSP boundaries.
 - Stronger tools to fight **spam, spoofing and fraud** once IP interconnection and authentication frameworks are aligned.

Proposed methodology for implementation in India

A phased, governance-heavy roadmap aligned to TRAI's current consultations

TRAI's ongoing consultation on IP-based interconnection and QoS already opens the door. A practical roadmap could look like this:

Phase 0 – Foundation (0–12 months)

1. Interconnection Policy Statement & Principles

- Issue a consolidated “**IP Interconnection & QoS Framework for India**” setting principles:
 - Technology-neutral but IP-oriented;
 - Non-discrimination;
 - Cost-orientation with a glide path to bill-and-keep where feasible;
 - Consumer-centric outcomes (QoS, affordability, security, transparency).

2. Technical Baseline

- Through a TRAI/DoT technical working group, adopt **reference SIP/IMS profiles, ENUM schema, IPv6 requirements and QoS classes**, drawing directly from IMDA, ETSI and ITU experience.

3. Regulatory Mapping

- Map existing IUC, RIO regulations, and QoS regulations onto the new IP primitives, identifying which provisions are:
 - **Maintained** (e.g., non-discrimination),
 - **Re-expressed** in IP terms (e.g., POIs, QoS),
 - **Sunset** (TDM-specific constructs).

Phase 1 – IP-capable RIOs & QoS (Year 1–2)

1. IP-native RIOs for SMP operators

- Mandate that all operators with **SMP in interconnection or termination** publish IP-capable RIOs (like Singtel’s IP RIO), covering:
 - IP POI locations,

- SIP/IMS specs, security, redundancy,
- QoS classes and measurement methods,
- Processes (fault handling, capacity planning),
- Commercial terms (including IUC evolution).

2. QoS for IP interconnect

- Finalise QoS parameters for IP interconnection (latency, jitter, packet loss, availability, call setup success ratio) as hinted in TRAI's consultation, and integrate them into licences and RIOs.

3. ENUM & portability

- Establish a regulated **ENUM/central routing database** for number portability, ensuring uniform use by all TSPs for IP routing (following Singapore/Japan lessons). **Phase 2 – Migration & economic model (Year 2–4)**

1. Mandatory IP for new interconnections

- From a fixed date (say, **+24 months**), require that **all new interconnects** between networks (including 5G/VoLTE/VoWiFi) be IP-based; TDM can remain only as legacy fall-back, with no new TDM POIs permitted.

2. Glide path for termination charges

- Announce a **multi-year glide path** toward lower, symmetric mobile/fixed termination rates, with explicit review points to assess the feasibility of **domestic bill-and-keep** (referencing FCC and EU experience).
- Treat high-cost segments (rural, satellite/NTN) separately with targeted cost-based support rather than high, uniform IUC.

3. Security & anti-fraud integration

- Mandate IP-level authentication frameworks (STIR/SHAKEN-like) for interconnect SIP trunks, integrated with India's UCC/robocall regime, leveraging the fact that IP interconnection simplifies end-to-end identity assurance.

4. Pilot and sandbox

- Establish a **regulatory sandbox** for innovative interconnect models (e.g., API-based interconnection with CPs, slicing-based QoS for enterprise/IoT) with relaxed rules but strict consumer-protection safeguards.

Phase 3 – Consolidation & holistic interconnection (Year 4–6)

1. Review and consolidate regulations

- After large-scale IP adoption, TRAI should **consolidate legacy IUC, interconnect and NGN documents into a unified “Interconnection Code”**, similar to EU's consolidation under the EECC and Singapore's Telecom & Media Competition Code.

2. Extend interconnection principles to new domains

- Apply proportionate, competition-safe interconnection principles to:
 - **CP/CDN traffic** (learning from South Korea's experience but avoiding innovation-chilling usage-fees),
 - **Satellite/NTN, IoT, 5G slices,**
 - Future **non-voice traffic classes** where QoS or resilience is critical (emergency alerts, health, critical infrastructure).

3. Outcome-based consumer KPIs

- Publish annual “**Interconnection & QoS Scorecards**”: call completion rates, inter-operator QoS, number portability times, outage handling, robocall complaint statistics—operator-wise but also aggregated—to keep consumer pressure aligned with regulatory goals.

Governance, transparency & collaboration mechanisms

- **Interconnection & QoS Board (IQB)**

Set up a standing expert group under TRAI/DoT comprising TSPs (including small ISPs), equipment vendors, consumer organisations (like your VCO), and academia to:

- Maintain technical reference profiles (SIP, ENUM, IPv6, security),
- Advise on QoS standards and measurement,
- Periodically recommend updates to the Interconnection Code.

- **Mandatory publication & open data**

- Require operators to publish RIOs, IP POI lists, and key QoS metrics in **machine-readable formats**, enabling civil society and researchers to build independent dashboards and analyses (a lesson from EU/ACCC transparency practices).

- **Time-bound dispute resolution**

- Create a **fast-track interconnection dispute process** with strict timelines (e.g., 30–60 days) and interim relief powers, mirroring IMDA/ACCC styles, so that smaller operators and new entrants are not blocked by commercial stalemates.

- **Consumer-facing communication**

- As each phase is rolled out, TRAI and DoT should publish simple, multilingual explainers:
 - what IP interconnection means,
 - expected benefits (better call quality, fewer spam calls), and
 - mechanisms for consumers to complain when QoS/security commitments are not met.

In summary

The **best global models** (EU, US, Singapore, Australia, Korea, Japan) converge on three ideas:

1. **All-IP interconnection with clear QoS and security expectations,**
2. **Economic rules (cost-orientation / bill-and-keep) that minimise arbitrage and support competition, and**
3. **Transparent RIOs and rapid dispute resolution to protect smaller players and, ultimately, consumers.**

For India, the challenge—and opportunity—is to embed these into a **phased, governance-heavy roadmap** that leverages our strong IPv6 adoption, 4G/5G penetration and digital-public-infrastructure experience, while keeping consumer empowerment and long-term sustainability at the centre of every interconnection decision.

Q36. Kindly mention any other challenges or concerns related to the regulations being reviewed in this consultation paper. Note: 1. All principal regulations referred to in this consultation paper should be read together with their subsequent amendments, as issued from time

to time. 2. For all purposes, the Gazette notifications of regulations and their amendments mentioned in this consultation paper may be referred to.

Comments :

1. Technology advancement – where the legacy framework is showing its limits

Here the key point is: *even after all amendments, the nine regulations are still TDM/LSA-era constructs*, and not fully aligned with IP/5G/6G, cloud, satellite and cyber-security realities.

(a) IP-based interconnection & IMS/SIP migration

Challenges / concerns

1. TDM bias across the legacy stack

- The core interconnection instruments – *Register of Interconnect Agreements Regulations, 1999; Port Charges, 2001; Charges & Revenue Sharing, 2001; IUC, 2003; RIO, 2002; BSNL transit, 2005; IN Services, 2006; SMS Termination, 2013; and Interconnection Regulations, 2018 with the 2020 amendment* – all evolved around TDM, E1 trunks and circuit-switched POIs.
- While the **2018 Interconnection Regulations** and **Second Amendment 2020** introduced some flexibility on POI levels, they still do not define IP-layer concepts like SIP interconnect profiles, codec negotiation, or packet-level QoS and measurement.

2. No single, binding IP-interconnection baseline

- TRAI's past *Consultation Note on IP-based Interconnection (2015)* and current 2025 Consultation Paper again examine IP interconnect, but outcomes are scattered and voluntary.
- There is **no consolidated, gazetted "SIP/IMS interconnection profile"** analogous to 3GPP/ETSI inter-operator profiles, leading to proprietary bilateral arrangements, interoperability issues and avoidable disputes.

3. ENUM, MNP and number-based OTT calling

- The framework assumes E.164 numbers mapped to physical networks; but consumers increasingly use **VoLTE/VoWiFi and number-based OTT voice**. There is no clear ENUM-style or equivalent mapping framework in the interconnection regulations to ensure correct routing, caller identity and QoS for number-based IP calls, especially across MNP boundaries.

4. 5G SA, network slicing and edge-POIs

- The consultation paper explicitly flags 4G/5G and 6G and satellite networks as drivers for review, but the current regulations:
 - Do **not recognise network slices** with differentiated QoS (e.g., URLLC vs mMTC) at interconnection points.
 - Assume POIs at LSA/district level, whereas **5G SA uses MEC/edge nodes** and may require *local* interconnection near where traffic originates/terminates (e.g., industrial campus, smart city).

5. Cloud-native cores & virtual POIs

- The regulations assume **physical POIs** and fixed MSC/SDCC type switching centers. With 5G/6G, many operators run **cloud-native cores (CUPS, SBA)** and virtualized SBCs in multiple clouds.
- No clarity exists on:
 - Whether **logical/virtual interconnection points** are acceptable “POIs”;
 - How to regulate capacity, congestion and QoS for traffic that traverses multiple public or private clouds;
 - How to record such POIs in the *Register of Interconnect Agreements*.

(b) IPv6, QoS classes and measurement

6. IPv6 not embedded in interconnection obligations

- TRAI has separate IPv6 initiatives, but **interconnection regulations do not mandate IPv6 support** at interconnect interfaces or require dual-stack capability.
- Without IPv6-ready interconnect, consumers may face degraded performance for IPv6-only content and emerging IoT services.

7. QoS defined only at service level, not at interconnect level

- Current QoS regulations and POI congestion reports focus on **E1 utilisation and call blocking**, not on IP-metrics like **packet loss, latency, jitter, MOS, 95th/99th percentile performance**, etc.
- As traffic becomes predominantly data/IP, **QCI/5QI and QoS class mapping across operator boundaries** is not

standardized, so one operator's "HD voice" or low-latency slice may not be honoured end-to-end.

(c) Cybersecurity & lawful intercept modernization

8. Interconnection not aligned with new cyber security rules

- The **Telecommunication Cyber Security (TCS) Rules, 2025** focus on mobile number validation, device traceability and sharing telecom-identifier data to fight fraud.
- However, interconnection regulations **do not yet embed** obligations for:
 - Authenticated CLI / verified calling across networks;
 - Anti-spoofing protections at POIs;
 - Cooperative data sharing for fraud analytics (within privacy limits);
 - Joint handling of compromised networks or DDoS events.

9. Lawful Intercept (LI) in encrypted & OTT-rich environments

- LI obligations were framed around circuit-switched voice and SMS. Now, with **VoLTE, VoWiFi, SRTP, TLS, and end-to-end encrypted OTT**, LI cannot be assured solely at traditional POIs.
- There is **no explicit articulation** in interconnection regulations of:
 - How LI coordination should work between IP POIs, satellite earth stations and OTT gateways;
 - How to handle LI for cross-border cloud-hosted application servers.

10. Resilience against outages and disasters

- While TRAI separately works on emergency telecom, interconnection regulations **do not codify resilience requirements** such as:
 - Minimum redundancy and geo-diversity of POIs;
 - Priority routing for emergency and critical communications;
 - Obligations to restore interconnection within specified timelines after large-scale outages.

2. Industry changes – structural and market challenges the current regs don't fully cover

(a) Market consolidation & SMP risk

11. Highly concentrated market vs multi-operator assumptions

- The early regulations (IUC, revenue sharing, BSNL transit etc.) assumed **many symmetric operators**. Today, India is effectively a **highly concentrated tri- or quad-play mobile market**, and BSNL/MTNL's role has changed.
- Existing provisions on **non-discrimination and reciprocity** may not sufficiently address:
 - **Margin squeeze** risks between large MNOs and smaller access/ILD/ISP players;
 - Potential foreclosure of new entrants (e.g., enterprise 5G, private networks, satcom licensees).

12. SMP & RIO framework not tuned for IP / 5G

- *Reference Interconnect Offer (RIO) Regulations, 2002* and subsequent practice focus on TDM POIs and classical voice/SMS products.

- There is **no updated template RIO** for:
 - IP interconnect with SIP/IMS profiles;
 - Network slices (low latency, IoT, mission-critical);
 - Fixed-mobile convergence, VoWiFi roaming, or satellite-mobile gateways.

(b) OTT–Telco interconnection and A2P/enterprise traffic

13. OTT bypass vs fair contribution vs consumer choice

- OTT services carry huge volumes of **voice, messaging and video** but sit **outside the interconnection framework**.
- This leads to:
 - Continued disputes on whether OTTs should pay termination or contribute to network costs;
 - Lack of common standards for **spam control, CLI verification, and QoS** for OTT calls terminated on telco numbers;
 - Risks of **over-the-top blocking / throttling** unless a clear, net-neutral, interoperable framework is articulated.

14. A2P SMS and enterprise messaging

- *SMS Termination Regulations, 2013* and TCCCPR regime together govern charges and spam control.
- However, the **explosive growth of A2P/enterprise SMS, RCS and IP-based messaging APIs** raises new challenges:
 - Whether SMS termination charges and transactional charges remain cost-oriented;

- How to treat **IP-based A2P channels vs SMS**, and avoid arbitrage or consumer confusion;
- Ensuring fair access for small businesses and start-ups to messaging channels at non-discriminatory terms.

(c) Termination charges, bill-and-keep and international traffic

15. Domestic bill-and-keep implementation gaps

- Through successive amendments to IUC (up to the **Sixteenth Amendment 2020**), India has moved to **zero domestic mobile termination** and largely bill-and-keep.
- Remaining challenges:
 - Aligning **fixed-mobile, SMS and special services** with the bill-and-keep philosophy;
 - Ensuring that zero-MTC does not encourage **abusive traffic pumping** or off-net congestion;
 - Integrating **satellite and future NTN traffic** in a way that remains affordable for consumers but viable for high-cost networks.

16. International termination, roaming and 6G non-terrestrial networks

- International termination and roaming still rely heavily on bilateral commercial arrangements, with limited transparency for regulators or consumers.
- With **6G and non-terrestrial networks (NTN)** now in the policy horizon, international interconnection will involve **satellite**

constellations, global cloud PoPs, and new security norms, which current regulations don't anticipate.

(d) Dispute resolution, compliance and register of agreements

17. Slow, litigation-heavy dispute resolution

- Even where regulations set timelines for entering into interconnect agreements or augmenting POIs, actual disputes often migrate to **TDSAT and courts**, delaying resolution and affecting consumers.
- There is no **light-touch, time-bound interconnection ombudsman or arbitration mechanism** anchored in the interconnection framework.

18. Register of Interconnect Agreements – incomplete transparency

- The *Register of Interconnect Agreements Regulations, 1999* was visionary, but in practice:
 - Not all amendments/addenda are filed promptly;
 - The register is not easily searchable by service category, region, or effective date;
 - Public visibility is limited, especially on *technical* terms (e.g., IP interface specs, QoS commitments) versus purely commercial clauses.

19. Inconsistent implementation of congestion and augmentation rules

- POI congestion reporting exists, but **automatic triggers for mandatory augmentation, penalties and public disclosure** are not tightly embedded in the interconnection regulations.

3. Consumer benefits – why solving these issues really matters

For each of the above challenges, you can explicitly tie back to *consumer-facing outcomes*:

1. Affordability

- Clean, predictable frameworks for **termination charges and bill-and-keep**, extended coherently to IP, SMS, satellite and enterprise traffic, will:
 - Reduce hidden costs;
 - Enable **simpler, unlimited or bundled tariffs**;
 - Avoid off-net/on-net price discrimination that historically hurt low-income or rural users.

2. Reliability & resilience

- Defining **redundant, geo-diverse IP POIs, QoS thresholds and congestion triggers** ensures that even when one network or region fails, consumers can still reach emergency services and critical applications.
- A modern, IP-centric interconnection code would reduce dropped calls, failed OTPs, and service outages during disasters.

3. Portability and choice

- Better integration of **MNP, ENUM-like mapping, VoWiFi, satcom and OTT voice** in the interconnection framework will

preserve **number portability and service continuity** across technologies.

- Consumers can change operators or move across regions without losing reachability or call quality.

4. **Security, trust and fraud protection**

- Embedding **cyber-security and TCS Rules 2025 principles** into interconnection – verified CLI, secure signalling, joint fraud analytics – will:
 - Reduce spoofed calls and SMS fraud;
 - Improve the trustworthiness of **banking, e-commerce and e-governance OTPs**;
 - Protect vulnerable consumers from phishing and identity theft.

5. **Service quality & innovation**

- Standardised **IP interconnection profiles, QoS classes and slice-to-slice mapping** will enable:
 - High-quality **HD voice, low-latency gaming, telemedicine and remote education** across networks;
 - Wider innovation in **IoT, smart grids, connected vehicles**, etc., without each start-up having to negotiate bespoke interconnect terms with every operator.

6. **Transparency and empowerment**

- A modernised **Register of Interconnect Agreements + public dashboards** will:
 - Let consumers, civil society and researchers monitor whether operators comply with congestion, QoS and non-discrimination commitments;

- Build confidence that regulatory promises translate into real-world performance.

4. Proposed methodology for implementation – a phased, consumer-centric roadmap for India

Here you can propose a **structured roadmap** that respects ongoing investments, avoids shocks, but is clearly time-bound and aligned with the **Telecommunications Act, 2023** and new cyber-security rules.

Phase 0 (0–6 months): Mapping & principles

1. Consolidated mapping of the “Nine + Amendments” framework

- TRAI should publish an **official consolidation note** that:
 - Maps all nine interconnection regulations and their amendments;
 - Identifies overlaps, inconsistencies and obsolete provisions;
 - Tags each clause as “TDM-specific”, “technology-neutral”, or “candidate for IP-specific replacement”.

2. Statement of regulatory principles

- In parallel with the ongoing consultation, articulate **guiding principles**:
 - *Technology neutrality* with explicit recognition of IP/IMS, 5G/6G, satellite and cloud;
 - *Consumer primacy* (affordability, QoS, security);
 - *Simplicity and consolidation* – moving towards a single **Telecommunication Interconnection Code**.

3. Freezing new TDM-only obligations

- From a specified date, **avoid introducing any new regulation** that assumes TDM-only POIs unless justified for specific legacy scenarios.

Phase 1 (6–18 months): New Telecommunication Interconnection Code

4. Draft and notify a unified “Telecommunication Interconnection Code, 20XX”

- This Code would **replace**:
 - Interconnection Regulations 2018 (+2020 amendment);
 - IUC 2003 (+16 amendments);
 - RIO 2002;
 - Charges & Revenue Sharing 2001;
 - Port Charges 2001;
 - BSNL transit 2005;
 - IN Regulations 2006;
 - SMS Termination 2013;
 - Register of Interconnect Agreements 1999;

to the extent they remain relevant.
- Key elements to include:
 - **IP/IMS Interconnection Annex**: mandatory SIP profiles, codec sets, security (TLS/SRTP), IPv6, ENUM/number mapping and QoS metrics.
 - **POI & topology model**: physical and virtual POIs, recognition of edge/MEC, network slicing and satellite gateways.

- **QoS & congestion section:** packet-level metrics, 95/99 percentile thresholds, automatic capacity augmentation triggers.
- **Cyber-security & fraud control:** obligations for authenticated CLI, inter-operator cooperation under TCS Rules, incident disclosure to regulators.
- **LI coordination clause:** aligning interconnection with lawful intercept requirements in IP, satellite and cloud-native contexts.

5. Re-engineered RIO and Register regime

- Publish **standard RIO templates** for:
 - Retail voice/SMS interconnect;
 - IP data peering;
 - Enterprise/A2P services;
 - Satellite & NTN interconnect.
- Upgrade the **Register of Interconnect Agreements** to a **digital, searchable portal** with:
 - Versioned agreements and addenda;
 - Metadata tags (service type, technology, geography);
 - Public access for non-commercial terms and technical parameters;
 - Restricted but regulator-visible access for commercial details.

6. Timelines & transition for existing agreements

- Mandate that within **12–18 months of Code notification**, all existing interconnect agreements must either:
 - Be migrated to **Code-compliant templates**, or

- Seek **specific regulatory exemptions** with robust justification.

Phase 2 (18–36 months): Progressive IP-first implementation

7. Mandatory IP interconnection in high-traffic domains

- For metropolitan and high-traffic LSAs, set a date by which **all new or renewed interconnections must be IP-based**, with TDM retained only as a fallback.
- Require operators to report **IP vs TDM interconnect share**, with targets for progressive migration over 3–5 years.

8. Slice-aware and 5G/6G-ready interconnect

- Introduce a **slice classification and mapping table** in the Code (e.g., consumer broadband, enterprise mission-critical, IoT, emergency services).
- Require that inter-operator SLAs explicitly specify:
 - Slice types;
 - QoS guarantees;
 - Remedies in case of non-performance (credits, capacity augmentation, etc.).

9. Domestic and international termination reforms

- Re-examine **IUC and SMS termination** in light of bill-and-keep and OTT substitution, with a view to:
 - Maintaining **zero or near-zero domestic voice termination**;
 - Ensuring SMS and A2P charges remain **cost-oriented** and non-exploitative;

- Establishing **transparent bands** or caps for international termination that prevent grey-route arbitrage but protect consumers from excessive rates.

Phase 3 (36+ months): Continuous review, sandboxes and convergence

10. Regulatory sandboxes for new interconnection models

- Set up **interconnection sandboxes** for:
 - 6G/NTN pilots;
 - Cross-border cloud-hosted services;
 - Innovative OTT-telco collaboration (e.g., verified caller ID, emergency alerts, RCS).

11. Five-year rolling review mechanism

- Make it explicit in the Code that **interconnection regulations will be reviewed at least every five years**, with mandatory stakeholder consultations and consumer impact assessments.

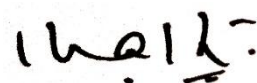
Governance, audits and transparency

12. Multi-stakeholder working groups

- Constitute permanent or long-term **Interconnection Working Groups** involving:
 - Access, NLD, ILD, ISP and satcom operators;
 - OTT communication providers;
 - Standards bodies (TSDSI, 3GPP liaison);
 - Consumer organisations and civil society;
 - Cyber-security and LI agencies.

- These groups can develop **technical annexes** (SIP profiles, QoS metrics, security options) that TRAI can adopt by reference, ensuring faster updates than full regulation amendments.
13. **Public dashboards and open data**
- Extend TRAI's existing **POI congestion and QoS reports** into an integrated **Interconnection Transparency Dashboard** that publishes:
 - POI congestion and augmentation timelines;
 - Share of IP vs TDM interconnections;
 - Interconnect-related outages and restoration times;
 - Key statistics on disputes and their resolution timelines.
14. **Compliance audits and enforcement**
- Mandate **periodic technical and financial audits** of interconnection compliance by independent auditors empanelled with TRAI.
 - Provide for **graded enforcement** – advisories, corrective action plans, penalties and, in severe cases, restrictions on new interconnections – with clear linkages to consumer impact (e.g., chronic congestion, repeated failure of OTP delivery, or persistent spam from specific interconnect paths).

Thanks.



(Dr.Kashyapnath)
President

