Peer Risk Intelligence: Should You Peer With That ASN?

Route Sherlock - Open Source BGP Intelligence Tool | 30-Minute Talk with Live Demo

The Problem

Network operators make peering decisions based on PeeringDB profiles and gut feel. No open-source tool answers: **"Is this network safe to peer with?"**

The Solution: Route Sherlock

CLI tool combining RIPEstat + PeeringDB + BGPStream to generate quantified peer risk scores.

```
$ route-sherlock peer-risk AS13335 ╔════════════════════════ Peer Risk Score
═══════════════════════════╗ ║ 100/100 (100.0%) ║ ║ Risk Level: LOW ║ ║ Recommendation:
RECOMMENDED ║ ╚════════════════════════════════════════════════════════════════════╝ Category
Score Key Factors ─────────────────────────────────────────────────────────────────────
Maturity 20/20 PeeringDB registered, IRR as-set Stability 30/30 Stable routing behavior
Incident History 30/30 Multiple upstreams (2465) Policy 10/10 Open peering policy
Security 10/10 IRR registered, multiple transits
```

Scoring Algorithm

Category	Points	Factors
Maturity	0-20	PeeringDB, IRR, IX count
Stability	0-30	BGP update frequency
Incident History	0-30	Topology, redundancy
Policy	0-10	Open/Selective/Restrictive
Security	0-10	IRR, transit relationships

Risk Levels

Score	Level	Action
80-100	LOW	Recommended
60-79	MODERATE	Monitor closely
40-59	ELEVATED	Caution
0-39	HIGH	Not recommended

Real-World Validation: Cloudflare 1.1.1.1 Incident (June 2024)

```
$ route-sherlock peer-risk AS267613 # Eletronet - involved in incident
╔═══════════════════════════ Peer Risk Score ═══════════════════════════╗ ║ 72/100 (72.0%) ║ ║
Risk Level: MODERATE ║ ║ Recommendation: ACCEPTABLE WITH MONITORING ║
```

```
╚══════════════════════════════════════════════════════════════╝ Stability 5/30 High
churn: 1637 updates/day (-25) ⚠️ Warnings • High BGP churn detected: 1637 updates/day
```

✓ **Validation Result:** AS267613 (Eletronet), which caused the June 2024 Cloudflare hijack, is correctly flagged with MODERATE risk and high BGP churn warning.

Historical Backtesting

```
$ route-sherlock backtest 1.1.1.0/24 --origin AS13335 --time "2024-06-27 18:00" 🚨
Anomalies Detected: 329 #1 [HIGH] ROUTE LEAK Time: 2024-06-27T18:49:06 AS Path: 50763 →
1031 → 262504 → 267613 → 13335 📅 Timeline: First anomaly: 2024-06-27 18:49:06 UTC
Duration: 7.6 hours
```

✓ **Detected 2 minutes before** Cloudflare's reported incident start time (18:51 UTC). Correctly identified AS267613 and AS262504 in leak path.

Talk Outline (30 min)

- **Problem** (5 min) - Current peering decisions
- **Solution** (3 min) - Route Sherlock intro
- **Live Demo** (10 min) - peer-risk command
- **Algorithm** (5 min) - Scoring breakdown
- **Validation** (5 min) - Backtest demo
- **Q&A** (2 min)

Key Differentiator: No existing open-source tool provides peer risk scoring. BGPalerter/ARTEMIS handle real-time monitoring; Route Sherlock answers *"Should I peer?"* before you establish the session.

Data Sources: RIPEstat API, PeeringDB API, BGPStream (RouteViews/RIPE RIS) | **Optional:** Claude API for AI synthesis
Requirements: Python 3.11+, pybgpstream (for historical) | **License:** Open Source