Detecting whether there are multiple devices behind and single IP address enables a service provider to determine if a subscriber is violating their terms of service by sharing their Internet connection with multiple households.

To detect and estimate the number of devices behind a device performing NAT, PacketLogic supports two methods: TCP timestamp tracking and TCP port tracking. Using these two methods, PacketLogic can alert the operator when thresholds for device counts on a for a subscriber are exceeded. Line sharing enforcement is done using triggers based on LiveView Custom view matching criteria.

**HIGH-VALUE USE CASES**

PacketLogic solutions enable a variety of use cases that provide significant benefits to fixed and mobile broadband operators, including:

- **Device Count** Detecting the number of devices used in the home behind a residential NAT.
- **Tethering Detection** Separating out traffic originating from a mobile device from traffic generated by devices tethered behind it.
- **Enforcement** If the number of devices exceeds the threshold, PacketLogic can block/shape/notify for all traffic for the subscriber.

**KEY SYSTEM BENEFITS**

Detecting number of concurrent devices behind the NAT
- A mix of algorithms are used to provide a count of the estimated number of devices

See application usage per device
- LiveView splits out the traffic generated by the applications over the detected devices behind the single host

Limit number of concurrent devices
- Enforcement rules can be provisioned when a subscriber exceeds a defined number of detected devices

**LINE SHARING DETECTION AND ENFORCEMENT DEPLOYMENT ARCHITECTURE**

![Figure 1](https://example.com/image1.png)

- **Pre:** 5 devices detected sharing single host IP
- **Internet:**
- **PRE:**
- **Aggregator:**
- **Wireless router with NAT:**
- **LiveView:**

**Figure 1**

---

**Pages:**

1

**Organization:**

PROCERANetworks.com
PACKETLOGIC™
LINE SHARING
DETECTION AND
ENFORCEMENT

KEY TECHNOLOGY
TCP timestamp tracking
This method estimates the number of devices by tracking TCP timestamps. Each device behind a NAT’d device has a unique boot time and frequency. Each detected device will have an ID that is unique per PacketLogic System. This ID may change over time as ID’s timeout, merge or diverge. IDs are meant to be used by LiveView and Statistics collection, not for specific device enforcement as they are not persistent. This means that the PacketLogic System/Local Host needs to be included in statistics distributions related to line sharing.

TCP port tracking
This method is used to detect devices using Windows type operating systems which typically have TCP timestamp disabled and use sequential port allocation scheme within defined ranges. This method estimates the number of devices by tracking TCP source ports.

ABOUT PROCERA NETWORKS
Procera Networks, the global Network Intelligence company, is revolutionizing the way operators and vendors monitor, manage and monetize their network traffic. Elevate your business value and improve customer experience with Procera’s sophisticated intelligence solutions. For more information, visit proceranetworks.com or follow Procera on Twitter at @ProceraNetworks.