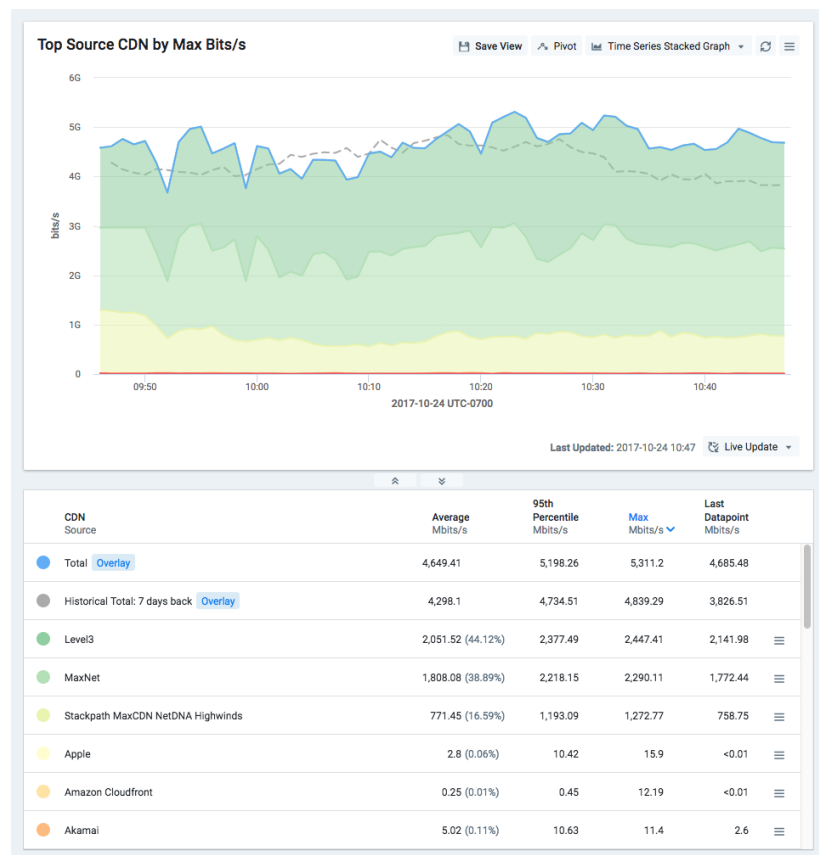# USING CDN ATTRIBUTION

KEY CAPABILITIES

- Full visibility into CDN traffic sources and distribution

- Trend CDN traffic growth over time

- Dynamic updates for IP-to-CDN mappings

- Proactive alerting based on CDN name

- Easy integration via APIs

KEY BENEFITS

- Make informed decisions on carrying CDN-sourced traffic.

- Negotiate based on real-world data to reduce transit and backbone costs.

- Quickly detect changes in CDN traffic volume or origin.

- Get automatic updates on CDN caches wherever they're deployed.

- Reduce MTTR (Mean Time to Repair) for congested links.

- Understand OTT market dynamics and detect new entrants.

- Evaluate CDN-related traffic in the context of your overall network traffic.

Content Delivery Networks (CDNs) deliver a large percentage of the traffic on the Internet today. While they've been around for years, the popularity of streaming services like Netflix, Hulu, and Amazon Prime has pushed the traffic volume from CDNs to a whole new level. As a result, Network Operations teams at both Service Providers and large Enterprises have seen an explosion in traffic on their networks. Identifying the CDNs associated with their traffic has long been a challenge for these teams, but it's gotten much easier with the introduction of the new CDN Attribution feature in Kentik Detect.
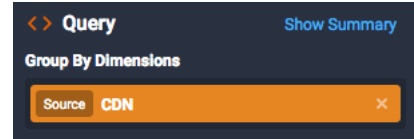
CDN Attribution Dimensions

| CDN Source	Average Mbits/s	95th Percentile Mbits/s	Max Mbits/s	Last Datapoint Mbits/s	
● Total Overlay	4,649.41	5,198.26	5,311.2	4,685.48	
● Historical Total: 7 days back Overlay	4,298.1	4,734.51	4,839.29	3,826.51	
● Level3	2,051.52 (44.12%)	2,377.49	2,447.41	2,141.98	☰
● MaxNet	1,808.08 (38.89%)	2,218.15	2,290.11	1,772.44	☰
● Stackpath MaxCDN NetDNA Highwinds	771.45 (16.59%)	1,193.09	1,272.77	758.75	☰
● Apple	2.8 (0.06%)	10.42	15.9	<0.01	☰
● Amazon Cloudfront	0.25 (0.01%)	0.45	12.19	<0.01	☰
● Akamai	5.02 (0.11%)	10.63	11.4	2.6	☰

CDN attribution makes it possible for Kentik Detect to determine whether a given flow record originated or terminated with a commercial CDN, and to store that information for each record using the following two columns of the Kentik Data Engine (KDE):

- `src_cdn`: The commercial name of the CDN derived from the source IP (`inet_src_addr`) of an ingested flow.

- `dst_cdn`: The commercial name of the CDN derived from the destination IP (`inet_dst_addr`) of an ingested flow.
  Note: This dimension enables you to track "fill traffic" that is pointed toward a CDN server to fill a local cache.

Once stored in KDE, the columns can be used for both group-by dimensions and filters in Kentik Detect queries (e.g. in Data Explorer, Dashboards, etc.) as described in Applying CDN Attribution.
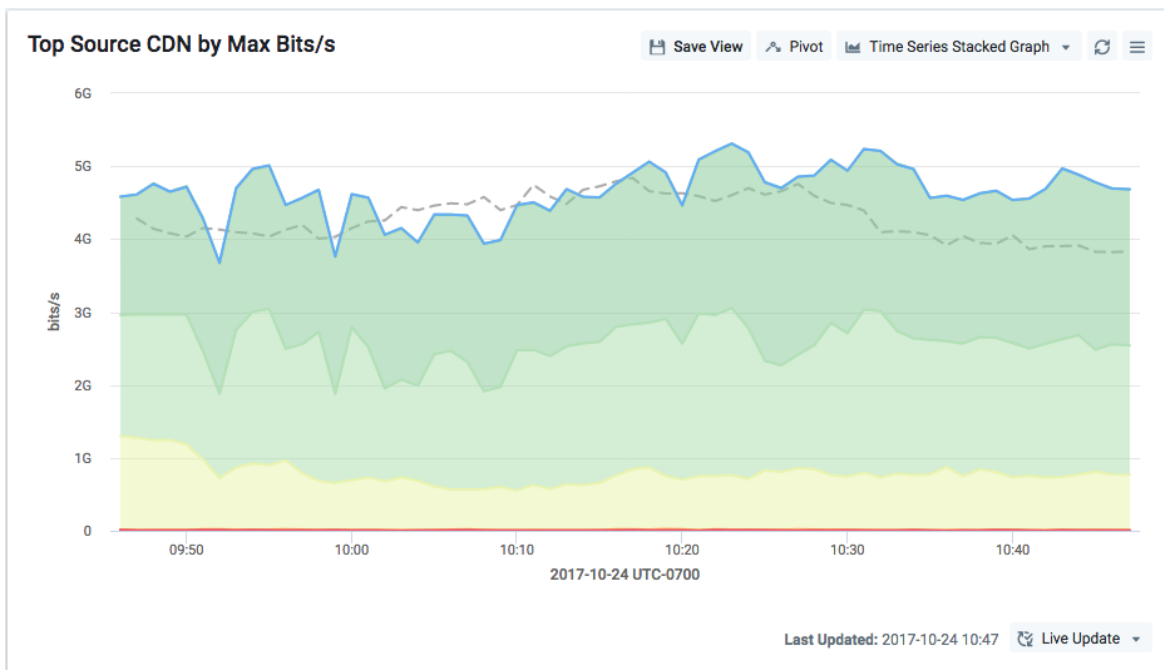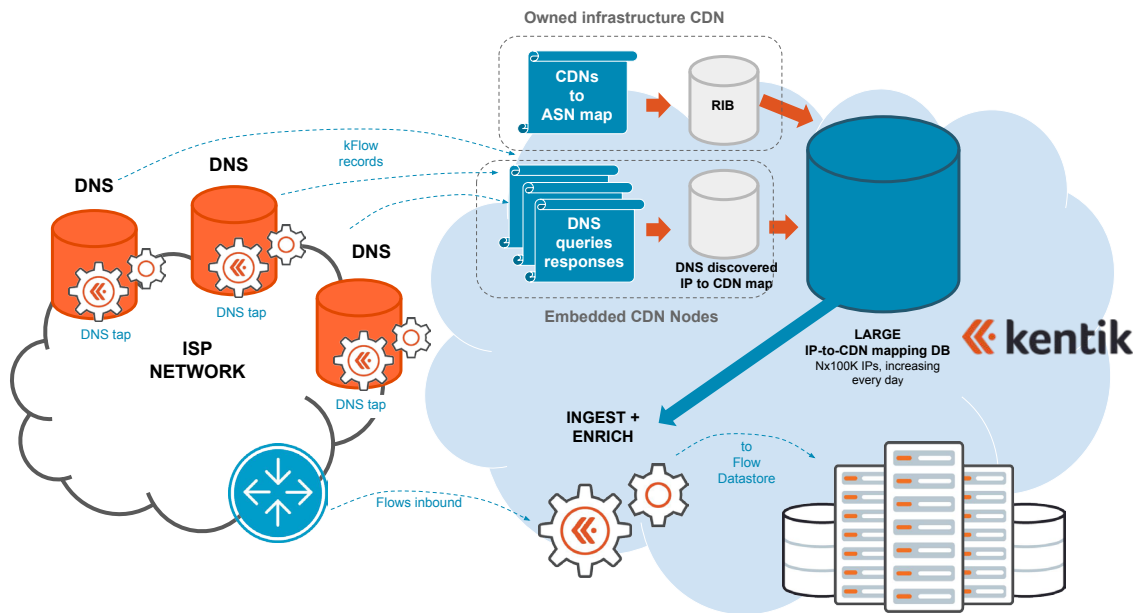

CDN Attribution Overview

While fairly simple in theory, mapping IPs to CDNs is non-trivial in practice, mainly because CDNs rely on two infrastructure scenarios:

- **CDN-owned Infrastructure**: Each CDN runs their own ASN(s), with their own PoPs running their own cache servers.

- **ISP-embedded infrastructure**: Many CDNs rely on ISP-embedded caching servers for better last mile performance. The CDN typically directs users of a given ISP to the CDN nodes that are co-located at the local ISP, closer to the end-users.

The above infrastructure scenarios may be blended in varying degrees by different types of CDNs, e.g. commercial, multi-tenant CDNs as distinct from single-purpose CDNs. But the dynamic algorithms employed by Kentik for CDN attribution allow IP mapping across the spectrum:

- A base mapping is obtained by listing ASNs by CDN and looking at their originated IP ranges.
- A more dynamic, additional layer taps into DNS traffic (upon ISP agreement) and deduces the remaining mappings.

The following diagram provides a simplified visual description of how CDN attribution operates:

Kentik has designed CDN attribution as a self-learning system that is updated once a day. The system constantly discovers new CDNs as they are born and new IPs (caching servers) as they are deployed.

Enabling CDN Attribution

Preparing your Kentik setup for CDN attribution involves the following tasks:

- Install our kprobe host agent software on at least one DNS server (see Host Configuration).
- Configure the corresponding kprobe device (in the Kentik Detect portal or via Kentik's Device API) to send DNS data to Kentik.

To configure CDN attribution in the portal:

1. Click **Admin** in the portal navbar, then choose **Devices** from the sidebar to open the Devices page.

2. Open the **Add/Edit Device** dialog:
   - If you want to register a new DNS server with Kentik Detect, click the **Add Device** button.
   - If you want to change the CDN attribution settings of an existing DNS server, click anywhere in the row corresponding to that device in the **Device List**.
   Note: Legacy nProbe devices (type host-nProbe-dns-www) can be set to contribute to CDN attribution (see step 4) but won't necessarily provide accurate information. To use CDN attribution, upgrade to kprobe as the host agent for all DNS servers (see kprobe Download and Install). If you need assistance with host agent software, please contact Kentik support (support@kentik.com).

3. If you're registering a new device, on the **General Settings** tab set **Type** to KPb (kprobe-beta).
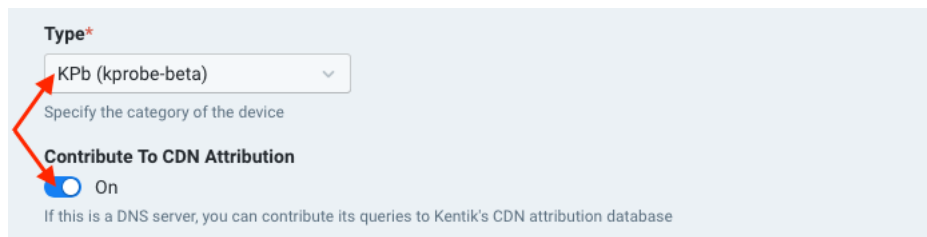

4. On the **General Settings** tab, set the **Contribute to CDN Attribution** switch to On.

5. Set the remaining fields on the dialog's tabs as needed (see About Device Fields).

6. Click the **Save** button. The dialog will close and you'll be back on the Devices page. If you added a new device it will now be shown in the **Device List**.

Note: DNS servers covering different geographical zones will typically result in distinct (largely non-overlapping) IP-to-CDN mappings. To export the best IP-to-CDN mapping data to KDE, Kentik recommends that CDN attribution users deploy kprobe on as many of their DNS servers as possible. This approach has the added advantage of providing highly granular NPM metrics for those devices.

Applying CDN Attribution

Once you've registered one or more DNS servers with Kentik and configured them for CDN attribution, the flow records stored for those devices in KDE will include the CDN Attribution Dimensions described above. You will now be able to use those dimensions in Kentik Detect queries:

- To use source or destination CDN as a group-by dimension, see Dimension Selectors.
- To use source or destination CDN as a filter (see screenshot below), see Filter Groups Interface.
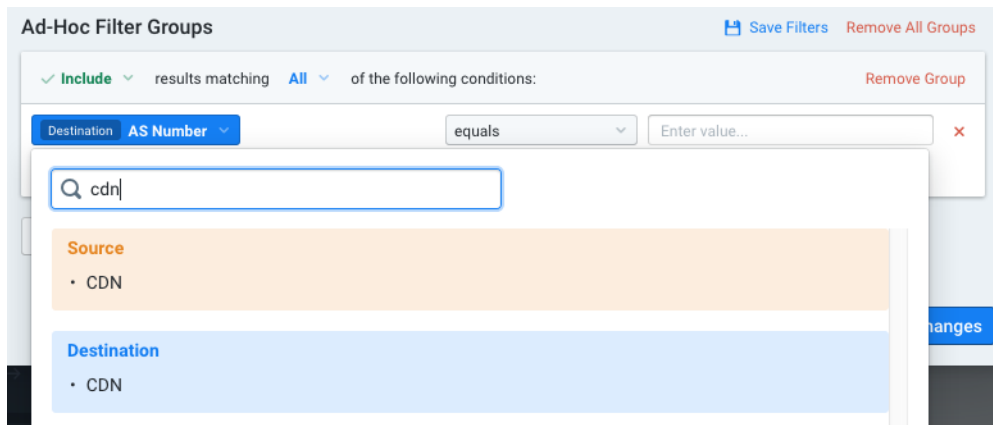
Using CDN for filters or group-by dimensions in Data Explorer or Dashboard queries can reveal (among other things) how much of your traffic is coming from (shown below) or going to various CDNs.

CDN Source	Average Mbits/s	95th Percentile Mbits/s	Max Mbits/s ∨	Last Datapoint Mbits/s	
● Total Overlay	4,033.19	4,551.65	4,722.8	4,008.89	
● Historical Total: 7 days back Overlay	3,198.38	3,658.17	3,817.78	3,307.82	
● Level3	2,954.95 (73.27%)	3,334.84	3,506.36	2,981.67	≡
● Stackpath MaxCDN NetDNA Highwinds	1,047.1 (25.96%)	1,214.79	1,271.04	1,004.17	≡
● Akamai	10.96 (0.27%)	33.23	37.53	11.17	≡
● Conversant - Reflected Networks - Swift	5.46 (0.14%)	21.43	28.07	4.98	≡
● Facebook	8.57 (0.21%)	13.99	20.73	6.7	≡
● Google Youtube	1.87 (0.05%)	6.23	13.41	0.12	≡

Alerting on CDN Attribution

Applying CDN Attribution not only allows you to query for CDN-related traffic, but also to create proactive alerts based on the source and destination CDN dimensions. That enables you to receive notifications when there are changes in the traffic patterns for all or a subset of the CDNs riding across your network infrastructure. For more on Kentik Detect's alerting capabilities, see our blog post on Kentik Detect Alerting.

Conclusion

Content Delivery Networks (CDNs) generate large volumes of traffic that are carried to end-users by Internet Service Providers (ISP) and Enterprises. Delivering this traffic can be expensive for these network operators, but for a long time they had no visibility into how much it was costing them. With Kentik Detect's CDN Attribution feature, ISPs and Enterprises can now see this traffic separately and determine its financial impact. Armed with that information, they are now able to make data-driven decisions and to negotiate with partners and providers to reduce overall costs.

ABOUT KENTIK

Kentik is the network traffic intelligence company. Kentik turns network traffic – billions of digital footprints – into real-time intelligence for both business and technical operations. Network operators, engineers, and security teams use Kentik to manage and optimize the performance, security, and potential of their networks and their business. To learn more about Kentik and its award-winning solutions, visit www.kentik.com.