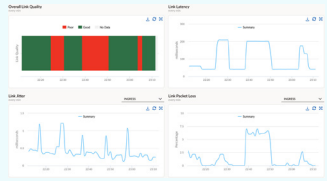
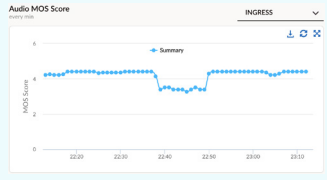
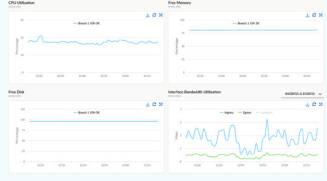

Prisma SD-WAN DVR and Reports

Prisma SD-WAN provides best-of-breed, actionable insights into network and application performance to help with network planning, resolving issues, and analytics. With granular telemetry that provides end-to-end visibility, you gain better control over business policies well-suited for your WAN network and applications to deliver the best user experience. The seven-day metrics that follow are included in the subscription license for the Prisma® SD-WAN Instant-On Network device and don't require additional SKUs or subscriptions.

Table 1: Prisma SD-WAN Instant-On Network Seven-Day Metrics

<p>Network Health and Usage Prisma SD-WAN gives you an instant overview of the device connectivity and health of each of your WAN links to see their utilization and performance</p>	<p>Dashboard</p>	<p>Understand device connectivity, top sites with issues, and summarized link quality</p>	<p>The top chart, 'Device To Controller Connectivity', shows a bar chart for Branch and Data Center connectivity. The Branch bar is at approximately 1400, and the Data Center bar is at 2. A legend indicates Online (green) and Offline (red). The bottom chart, 'Link MOS', shows a donut chart with a total of 1377 links. The legend indicates: 8 Bad (1-3.4), 8 OK (3.5-3.9), and 1361 Good (4-5).</p>
<p>Granular per Application Visibility Prisma SD-WAN provides top application usage across WAN links per application and session</p>	<p>Application Throughput</p>	<p>Visibility into the amount of throughput for a specific application</p>	<p>The chart shows bandwidth utilization in Mbps for Office365 Portal over time, with a peak around 22:30.</p>
	<p>Top Applications</p>	<p>See which applications are active on the network</p>	<p>A stacked area chart showing the usage of various applications over time, with Office365 Portal being the most prominent.</p>
	<p>Concurrent Flows</p>	<p>Understand how many connections are active on your network by application</p>	<p>The chart shows the number of concurrent flows for TCP and UDP over time, with TCP flows being significantly higher than UDP flows.</p>
<p>Application Response Time and Performance Prisma SD-WAN provides granular visibility into how your application performs, identifies cases where application transactions fail, and understands what factors contribute to these issues</p>	<p>Transaction Statistics</p>	<p>Identify successful and failed transactions per application session</p>	<p>The chart shows the number of transactions for Hit Successful, TTXs Successful, Hit Failure, and TTXs Failure over time.</p>
	<p>Application Quality and Health</p>	<p>Overview of user experience for a given application</p>	<p>The chart shows the health status of Office365 Portal, with metrics for Good, Partially Good, Unrecoverable, and No Data.</p>
	<p>Response Time Analytics</p>	<p>See the distribution between round trip time, network transfer, and server response time to identify the source of poor performance</p>	<p>The chart shows response time in milliseconds for WERPOS, broken down into RTT, NET, and SER components.</p>

Table 1: Prisma SD-WAN Instant-On Network Seven-Day Metrics (cont.)

Real-Time Voice, Video, and Collaboration Quality Prisma SD-WAN provides quality metrics related to voice and video at your fingertips to understand the user experience and identify any issues with quality or dropped calls	Link Statistics	Gain visibility into the latency, jitter, and packet loss encountered	
	Mean Opinion Score (MOS)	Instantly see MOS for sessions on your network	
System and Interface Metrics Prisma SD-WAN provides device-level and interface-level visibility per ION device to understand any issues at the port or appliance	Interface and System Metrics	Gain visibility into LAN traffic and identify potential errors and dropped packets Insights into CPU, disk, and memory utilization for devices	

Alongside these benefits, take advantage of our deep SD-WAN analytics over an extended period of time while generating detailed reports for offline access and reviews with these additional licenses:

- **Prisma SD-WAN DVR license:** With this license, you can access up to 90 days of statistics, policy, configuration, alarms, and alerts. This license applies per ION device.
- **Prisma SD-WAN Report license:** With this license, you have access to auto-generated and downloadable reports, providing network operators insight across various dimensions of their entire Prisma SD-WAN application layer. For example, utilization trends and hotspots reports help customers determine if they need to do circuit upgrades or simply adjust their policies.

Prisma SD-WAN DVR License

With a comprehensive real-time and historical view of your network and application performance, you can gain better insight into traffic outliers and network anomalies that help with better capacity planning, troubleshoot quicker, and improve compliance posture. The DVR license increases access to data and insights for a longer time period.

	Prisma SD-WAN	Prisma SD-WAN DVR
Data Availability on Dashboard	7 days	90 days
Data Granularity	1 hour (1 min.) 1 day (5 min.)	1 hour (1 min.) 1 day (5 min.) 1 week, 1 month (1 hour) 3 months (1 day)
Audit Logs & Configuration History	30 days	1 year
Events	30 days	1 year

Figure 1: Prisma SD-WAN DVR extended analytics

Prisma SD-WAN Report License

Prisma SD-WAN's reporting engine provides auto-generated report packages, giving IT administrators insight into the health, security, and performance of their WAN network and applications.

The **WAN Clarity Report package** is the first in a series of reporting packages delivered by the Prisma SD-WAN Reporting engine. This package gives network operators insights into utilization trends across various dimensions of their entire Prisma SD-WAN application layer.

The reports in this package help IT administrators understand the following requirements:

- Sites that potentially need a WAN circuit upgrade or downgrade
- Durations during which particular sites have highly utilized WAN links
- Occurrences of high utilization
- Top consumers of bandwidth based on an application, source IP, destination IP, and source and destination IP pair perspective

Having access to this wealth of data, IT administrators gain actionable insights to help with WAN capacity planning, network and QoS policy adjustments, and enforcement of proper use of network resources by their end user community.

	Report Type	Description
Branch Reports	Traffic Distribution	• Provides tenant-level summary of utilization across different WAN paths
	Utilization Quadrant	• Provides tenant-level summary of 90 th percentile utilization per site and circuit • Highlights sites and circuits that are possible candidates for resizing
	Utilization Over Threshold	• Provides daily breakdown of total time that utilization is over 70% of the provisioned bandwidth
	Heatmap	• Displays daily site and circuit utilization trend • Identifies the site local hours and days when circuit contention exists
	Hotspots	• Identifies top applications, source IPs, destination IPs, source and destination IP pairs, and undefined domains that contribute to contention on a circuit during hotspots
	Top N	• Identifies top applications, source IPs, destination IPs, source and destination IP pairs, and undefined domains for the entire week, not just during hotspots
	Application Volume per Circuit	• Provides a daily breakdown of application traffic per circuit

Figure 2: WAN Clarity Branch Report

In addition to the branch reports, the WAN Clarity Report package also includes reports specifically for data centers. The data center package consists of the following reports:

	Report Type	Description
Data Center Reports	Traffic Distribution	• Highlights utilization from top sites and applications from the data center's perspective in the form of Sankey charts
	Circuit Utilization	• Provides individual reports on ingress and egress utilization summary for each data center circuit • Identifies top branches, applications, source IPs, destination IPs, IP pairs, and undefined domains
	Hotspots	• Identifies top branches, applications, source IPs, destination IPs, source and destination IP pairs, and undefined domains that contribute to contention on a circuit during hotspots • For data centers, hotspots are generated for 90 th percentile circuit utilization
	Top N	• Identifies top branches, applications, source IPs, destination IPs, source and destination IP pairs, and undefined domains for the entire week, not just during hotspots

Figure 3: WAN Clarity Data Center Report

Branch Reports

This section provides an overview of the branch reports in the WAN Clarity Report package.

Traffic Distribution Report

The Traffic Distribution Report helps administrators understand utilization across different WAN path types at an application level. This report provides a quick overview of traffic distribution across the application layer, which can help ensure that aggregate path policy objectives are being met.

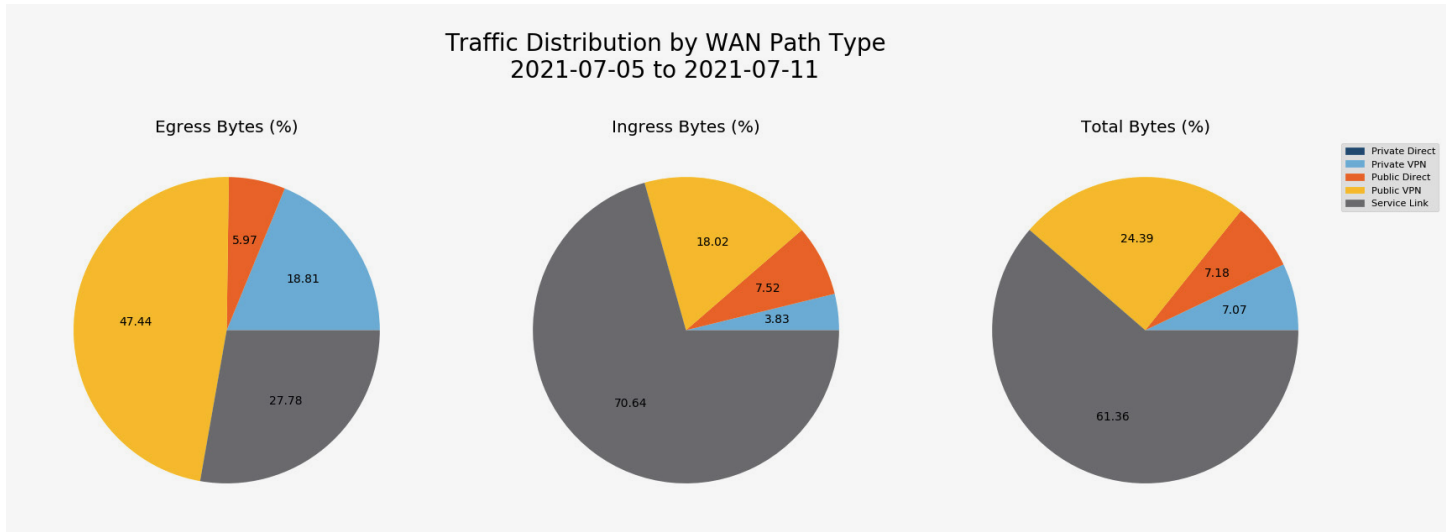


Figure 4: WAN Clarity Traffic Distribution Report

The sample chart above lists traffic distribution for a global enterprise for the week of July 5, 2021. This enterprise's objective of using more of their public WAN circuit types (e.g., broadband internet) versus their private WAN circuits (e.g., MPLS) is being met at an aggregate level. The following **Utilization Quadrant Report** will help identify which sites and circuits an administrator will focus on next.

Utilization Quadrant Report

The Utilization Quadrant Report offers a visual synopsis of circuit utilization for all sites. The report plots 90th percentile utilization for every circuit across the application layer, in both ingress and egress directions. The quadrant highlights circuits whose 90th percentile utilization is above 50% of the provisioned capacity in either the ingress or egress direction, thereby making it a candidate for further investigation. For example, if a particular site and circuit show up week after week, it may warrant adjustments to the circuit capacity. However, to assess whether the high utilization on a specific circuit is expected to carry business-critical traffic during business-impacting hours, an administrator may use the next set of reports to get more clarity and context on the utilization.

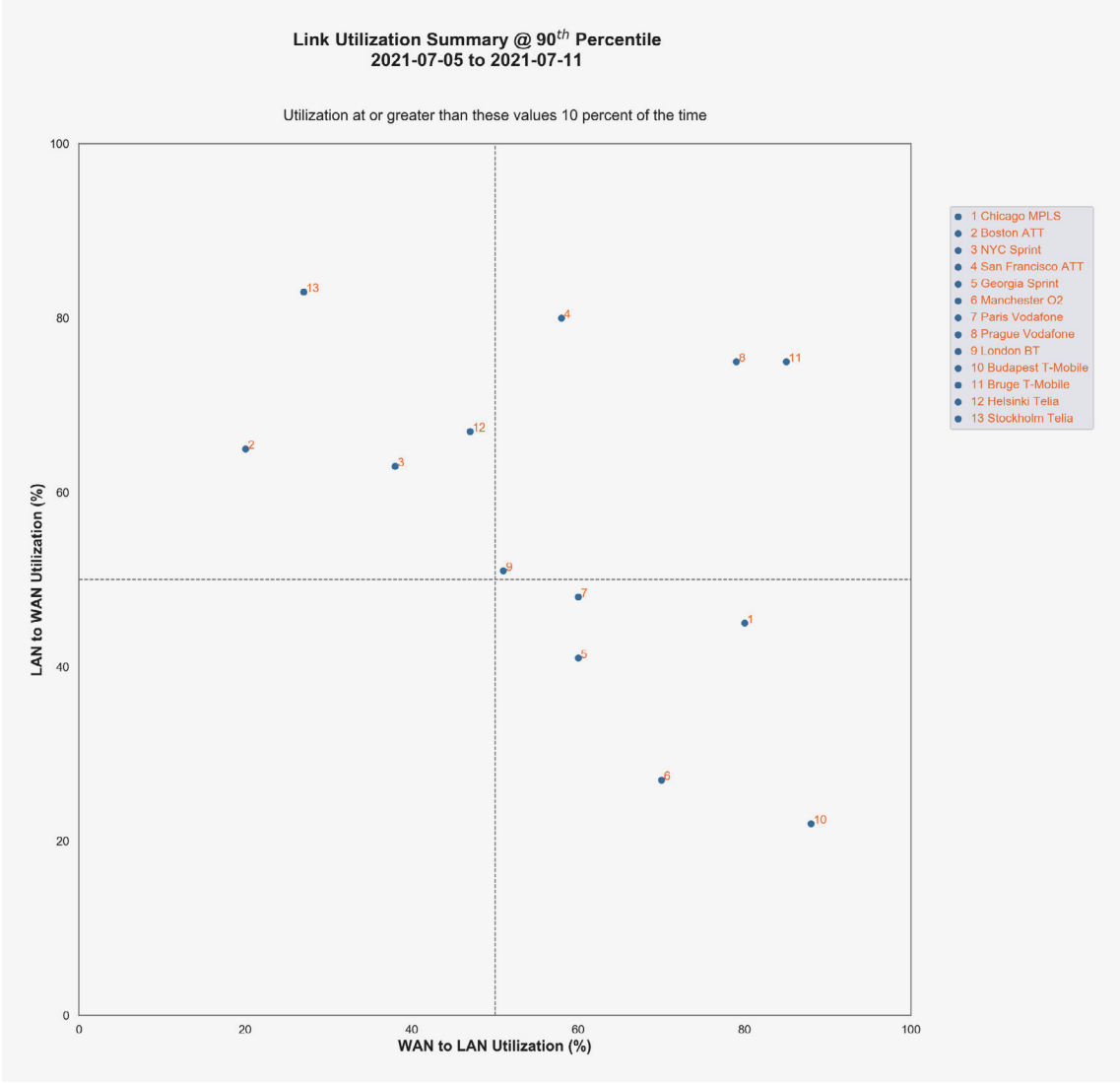


Figure 5: WAN Clarity Utilization Quadrant Report

The sample chart above summarizes utilization over a week for a global enterprise. 13 circuits stand out based on their utilization at the 90th percentile. One site and circuit to review further is the MPLS circuit in Chicago that seems to stand out for its egress utilization. The Utilization Over Threshold Report in the next section will provide more clarity as to the days and minutes when the MPLS circuit was highly utilized.

Utilization Over Threshold Report

The Utilization Over Threshold Reports are produced for any site and circuit present in the three quadrants of the Utilization Quadrant Report, representing greater than 50% utilization (at the 90th percentile). This report provides a daily aggregate of minutes when a circuit operates over the defined utilization threshold. For the initial WAN Clarity Report release, the threshold is set to 70%. This report supplements the Quadrant Report as it informs administrators of the days and the duration when a particular circuit exceeds that threshold.

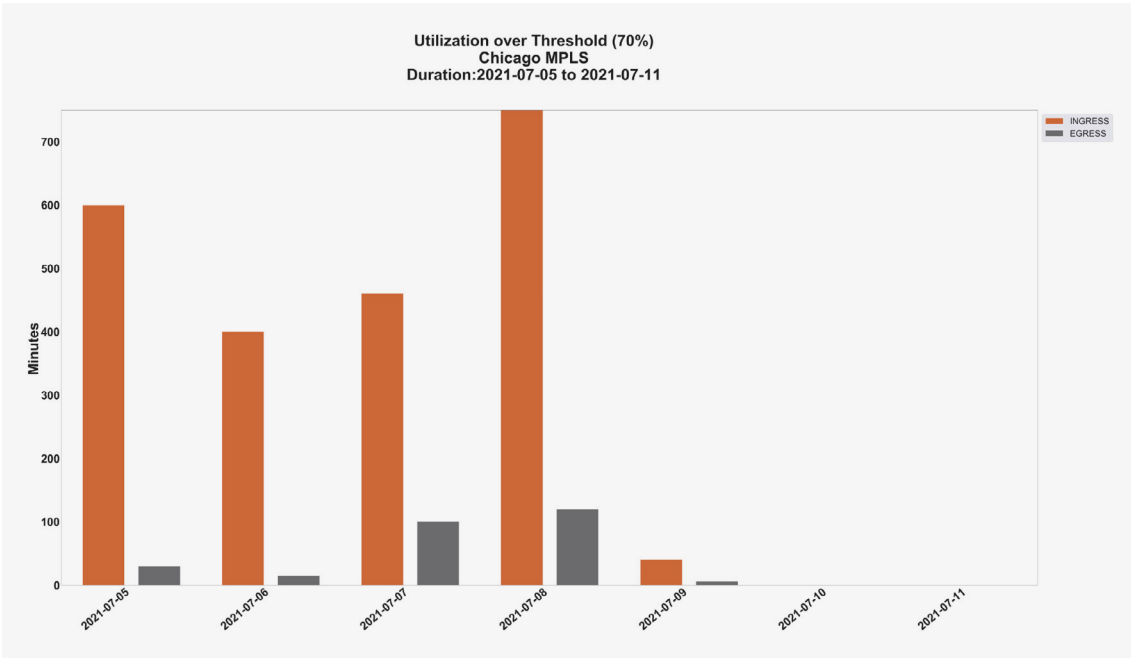


Figure 6: WAN Clarity Utilization Over Threshold Report

The sample chart above displays the total minutes when the Chicago MPLS circuit operated at or above 70% of the provisioned bandwidth. The majority of the high utilization is during the workweek and in the egress direction. However, to understand when the hotspots occurred during those days, review the Heatmap Report described in the next section.

Heatmap Report

The Heatmap Reports are produced for any site and circuit that is present in the three quadrants of the Utilization Quadrant Report, representing greater than 50% utilization (at the 90th percentile). This report provided more context to the hours of the day (site local time) when the high utilization occurred. If the observed contention mainly happens during business hours, an assessment of provisioned capacity may be warranted. The Heatmap Report also sheds light on abnormal bandwidth consumption behavior outside of regular business hours.

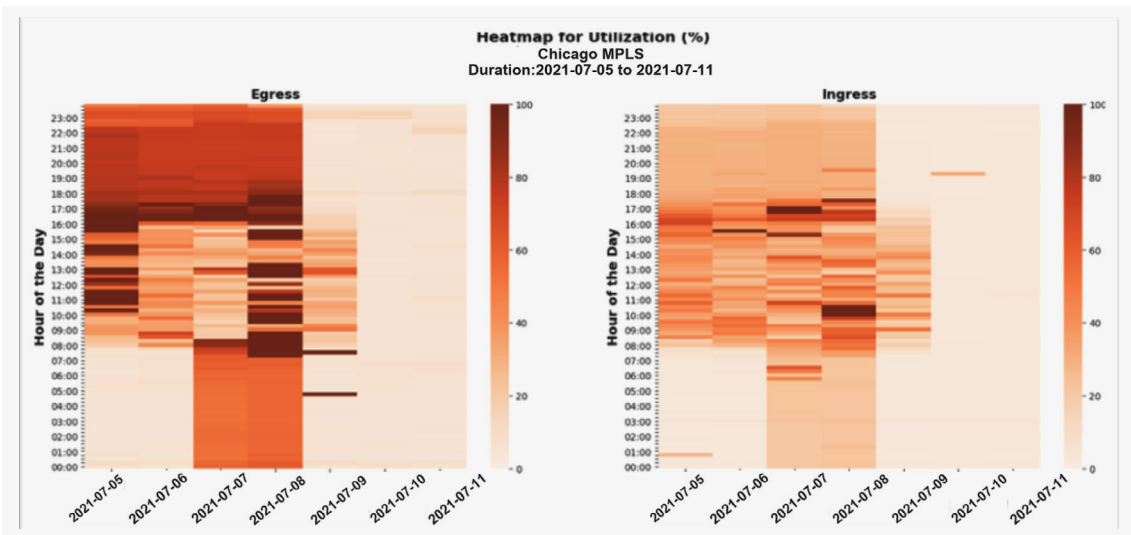


Figure 7: WAN Clarity Heatmap Report

The sample chart above shows the bandwidth consumption trend for the MPLS circuit in Chicago for one week. This chart is interesting as many more egress activities occur post business hours (after 1600 hours) than during business hours. This may not be anomalous if scheduled software upgrades, backup replication jobs, etc., typically happen after business hours.

However, there is also a good bit of contention between 2021-07-05 and 2021-07-11 during regular business hours. Suppose this trend is observed week after week. In that case, the network administrator should reassess the provisioned bandwidth on this circuit or rewrite application policies to load-balance traffic across multiple paths. The following set of Hotspot Reports will help identify which traffic contributes to the heavy load during these periods.

Hotspot Report

The **Hotspot Reports** are produced for each site and circuit with a corresponding Heatmap Report for granular insight into the circuits at the time of the hotspots. The accounts provide a list of applications, undefined domains, destination IPs, source IPs, and source and destination IP pairs observed during the hotspots.

A hotspot is any time period when the circuit utilization in either the ingress or egress direction is above 70% of the provisioned bandwidth. The charts generated for each Hotspot Report display the top 10, and a companion CSV file available within the package provides all of the data for each Hotspot Report.

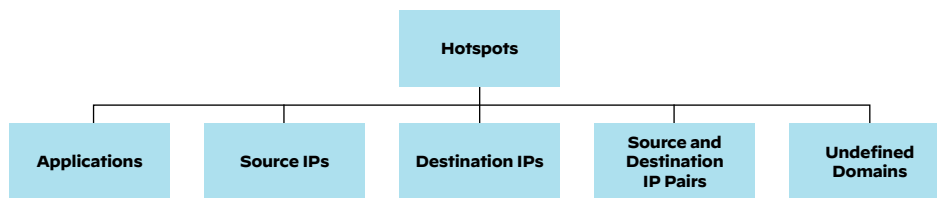


Figure 8: Hotspot Report

Hotspots: Applications Report

Once the hotspots in the heatmap have been identified, the **Hotspots: Applications Report** will clarify which applications contributed to the hotspots. First and foremost, the report can quickly give administrators insight into whether business-relevant applications consume bandwidth during hotspots. If the applications contributing most to high utilization are not business-relevant applications, this event will be less significant in assessing current WAN capacity. This information, however, can be instrumental in ensuring that the appropriate QoS and path policies are applied in the future to guarantee that business-critical applications are serviced first, with non-business-relevant applications potentially offloaded to alternate paths. If there is a trend of business-critical applications contributing to hotspots week after week, circuit capacity may be oversubscribed and will need to be reassessed.

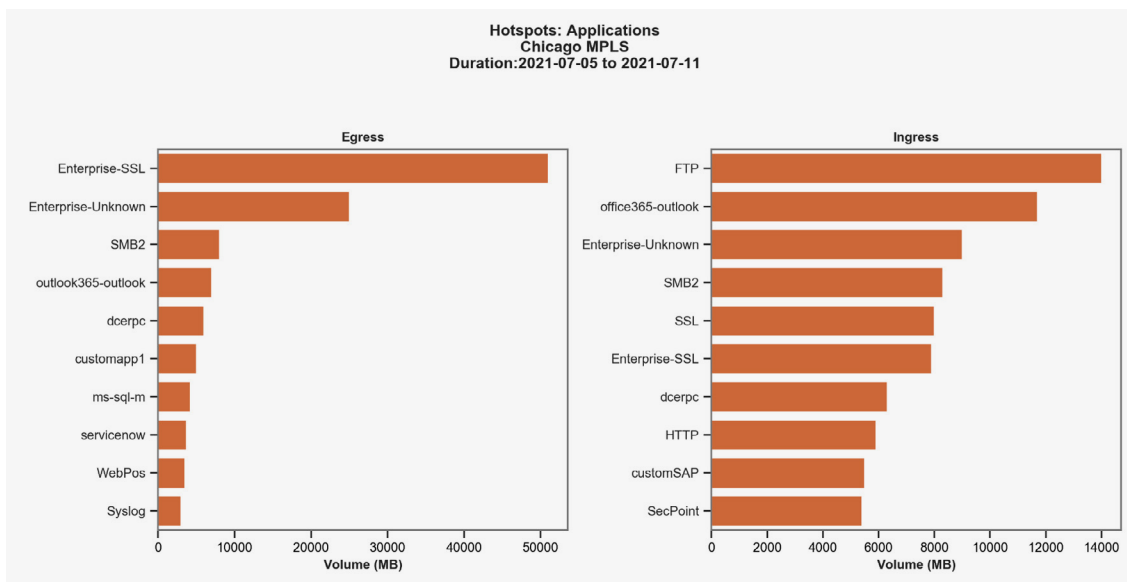


Figure 9: Hotspots: Application Report

The sample chart above lists the top 10 applications accessed during hotspots on the MPLS link in Chicago for one week. One of the takeaways from this report is the amount of traffic matching enterprise SSL and enterprise-unknown applications, which are generic catch-all applications for flows destined to enterprise prefixes: SSL and non-SSL (and non-HTTP), respectively.

The next set of reports around undefined domains and destination IPs can help clarify which enterprise FQDNs and IPs have the highest traffic to see if they are candidates for custom application creation.

Hotspots: Destination IPs Report

Based on the hotspots identified in the heatmap, the **Hotspots: Destination IPs Report** is generated to clarify which destination IP addresses contributed to the hotspots. This report is useful to correlate with the **Hotspots: Applications Report**, especially when the top application is a generic one like enterprise-unknown.

With these destination IP addresses, an administrator will have enough information to create a custom application so that they can apply unique QoS, WAN path, or security policies to these flows as needed, or at a minimum, define an application for purposes of utilization tracking and performance.

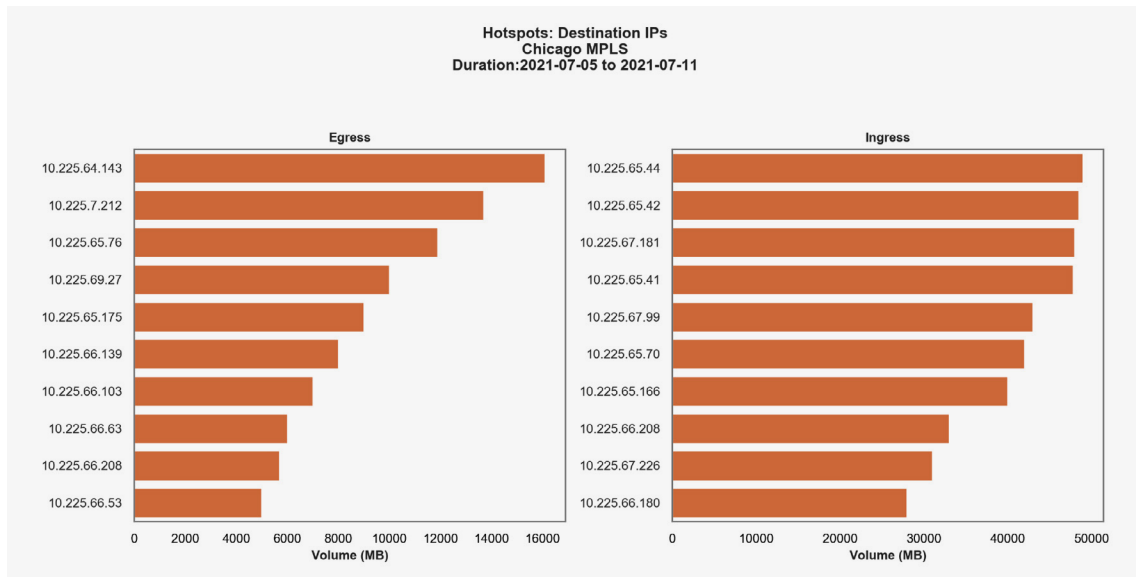


Figure 10: Hotspots: Destination IPs Report

The sample chart above lists the top 10 destination IP addresses accessed when the MPLS link in Chicago was hot.

Hotspots: Undefined Domains Report

The **Hotspots: Undefined Domains Report** lists the HTTP and SSL undefined domains observed during the hotspots. As these domains currently do not map to any system or previously defined custom application signatures, they may not be appropriately serviced. Rather, these domains will be observed in flows that match the generic application signatures of enterprise-SSL, enterprise-SSL, HTTP, or SSL.

This report is useful to correlate with the **Hotspots: Application Report**, especially when the top application is a generic one like enterprise-HTTP or enterprise-SSL. With these domains, an administrator will have enough information to create a custom L7 application definition to apply unique QoS, path, or security policies to these flows as needed, or at a minimum, define an application for purposes of utilization tracking and performance.

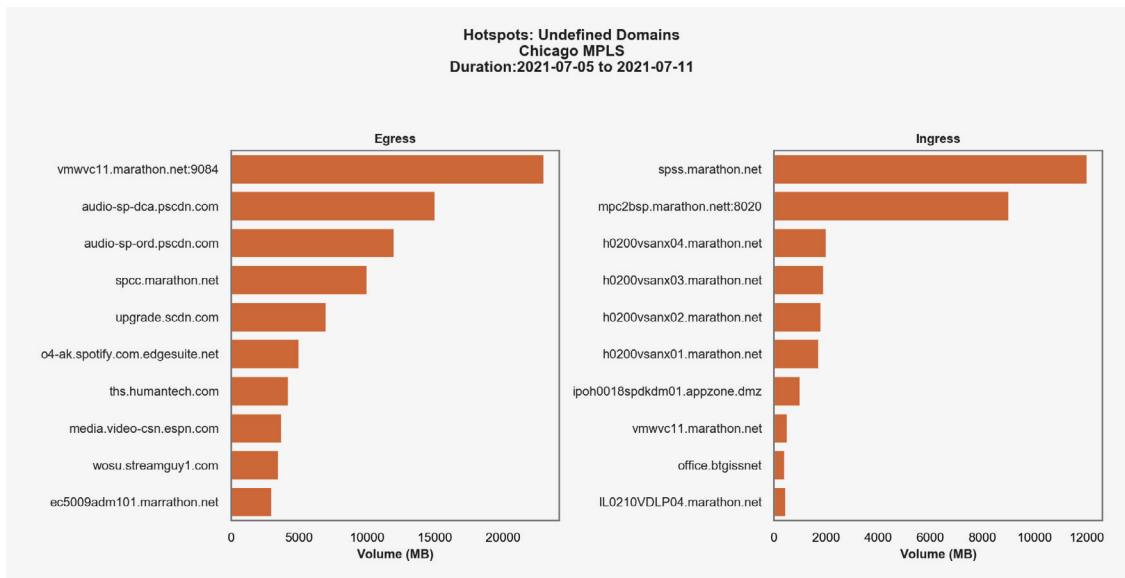


Figure 11: Hotspots: Undefined Domains Report

The sample chart above lists the top 10 domains accessed when the MPLS link in Chicago was experiencing a hotspot in either the ingress or egress direction.

Hotspots: Source IPs Report

The **Hotspots: Source IPs Report** helps administrators understand the consumption from an end user’s perspective. It sheds light on the top bandwidth consumers from a source IP perspective during the observed hotspot periods. This information can help filter out sources that may be contributing to unnecessary load on the circuit. For example, a server that is mis-scheduled to run backup replication jobs during regular business hours.

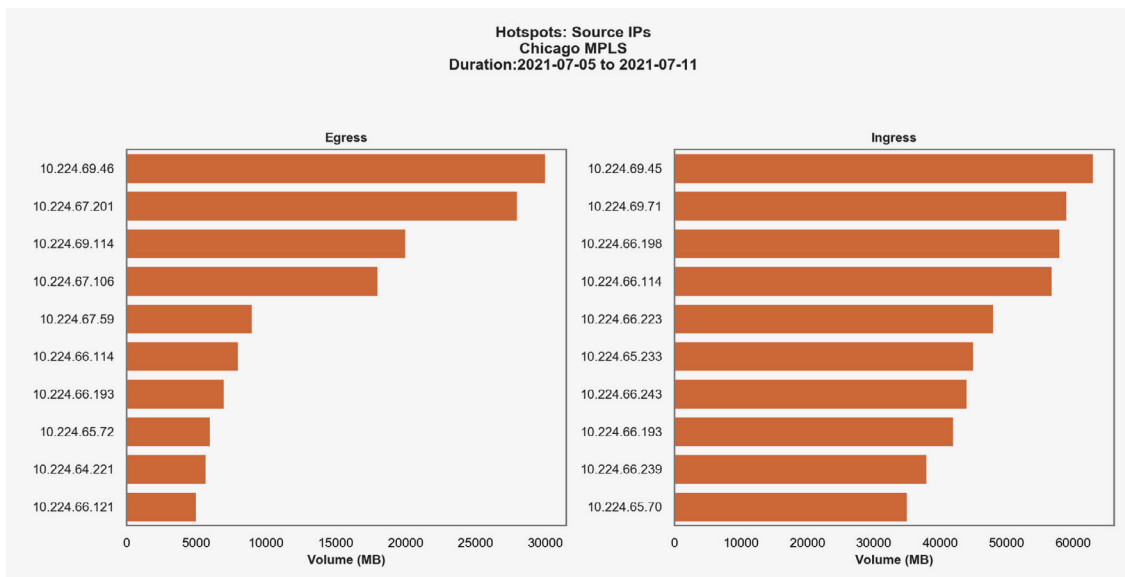


Figure 12: Hotspots: Source IPs Report

The sample chart above lists the IP addresses of the top 10 users who were active when the MPLS link in Chicago was experiencing a hotspot in either the ingress or egress direction.

Hotspots: Source IP–Destination IP Pairs Report

While the previous Hotspot Reports provided visibility into the most active origin and endpoints when the link was hot, the report, **Hotspots: Source IP–Destination IP Pairs Report**, lists the most active

source-destination IP pairs. This is useful in determining if the same set of source and destination IP pairs contribute to the contention week after week.

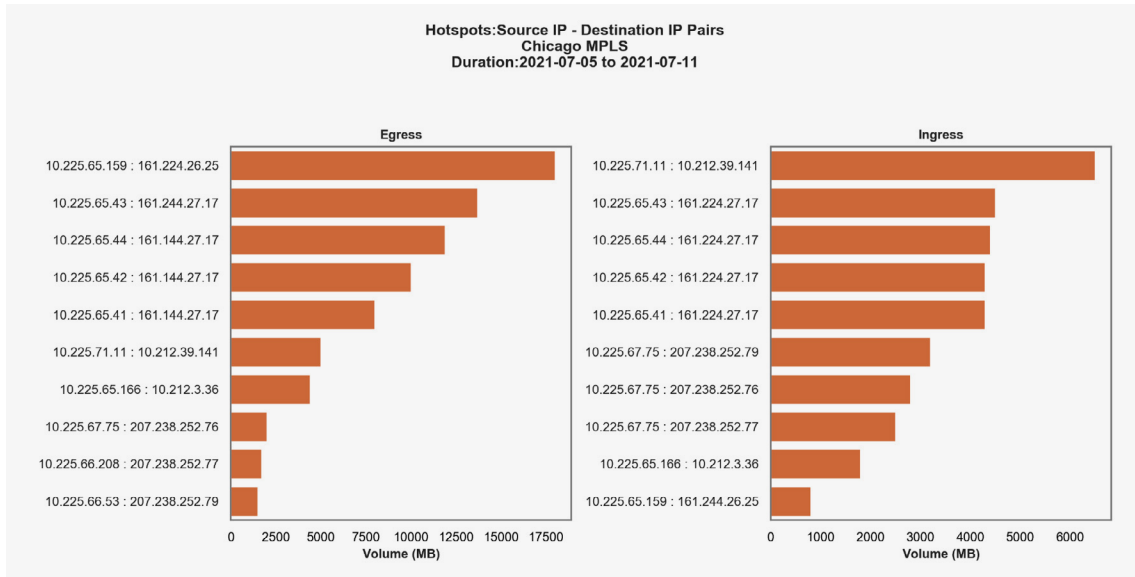


Figure 13: Hotspots: Destination IP Pairs Report

The sample chart above lists the top 10 source and destination IP pairs that were active when the MPLS link in Chicago was experiencing a hotspot in either the ingress or egress direction.

Top N Report

Top N Reports are a set of reports that provide insight into the top applications, source IPs, destination IPs, source and destination IP pairs, and undefined domains for the entire week. These reports are generated at a site level. They include a chart listing the top 10 of each category along with a companion CSV file with information about all the contributors in that specific category.

Insights from this report can be used to understand site-specific trends and turned into actions, such as changing path policies, changing application priorities, and reassessing the provisioned bandwidth for over-subscribed and under-utilized circuits.

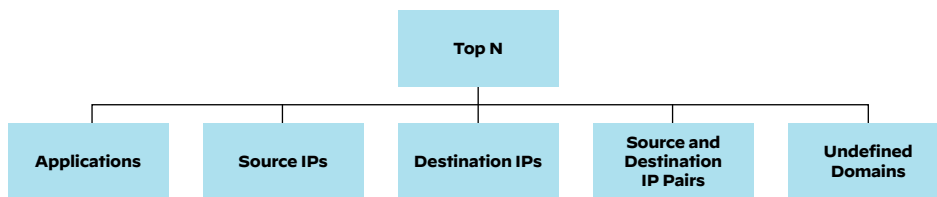


Figure 14: Top N Reports

Unlike the Hotspots Report, which only looks at flows that traversed the network during periods of hotspots, the Top N Report studies flow and application data for the entire week to determine which applications, users, and domains contribute the most to high bandwidth utilization.

As shown in the previous sections, sample reports for the Chicago branch for the same week are listed below.

Top N: Applications Report

The **Top N: Applications Report** lists the top applications for the entire week and is not limited to hotspots. This report is generated per site, unlike the Hotspots Application Report, which is specific to periods of hotspots (utilization over 70%) on a particular circuit.

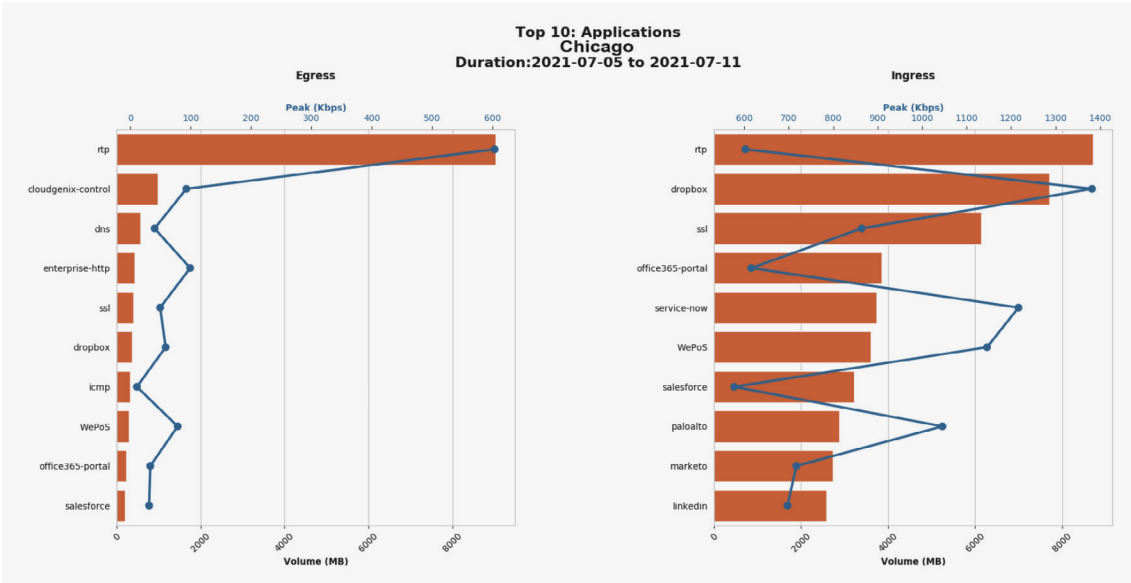


Figure 15: Top 10 Applications Report

The sample chart above lists the top 10 applications for Chicago across all circuits for the week. It is interesting to note that a similar set of applications are listed for the Hotspot: Applications chart for the Chicago MPLS circuit. This indicates that further refinement of application definitions is required, with possible path, QoS, and security policies.

Top N: Destination IP Report

The **Top N: Destination IP Report** lists the top destination IPs for the entire week and is not just limited to hotspots. This report is generated per site, unlike the Hotspots Destination IP Report, specific to hotspots (utilization over 70%) on a particular circuit. This report helps administrators understand the destination of most traffic during the week. One potential use case for this information could be the flagging of anomalous or ill-intended destination IPs.

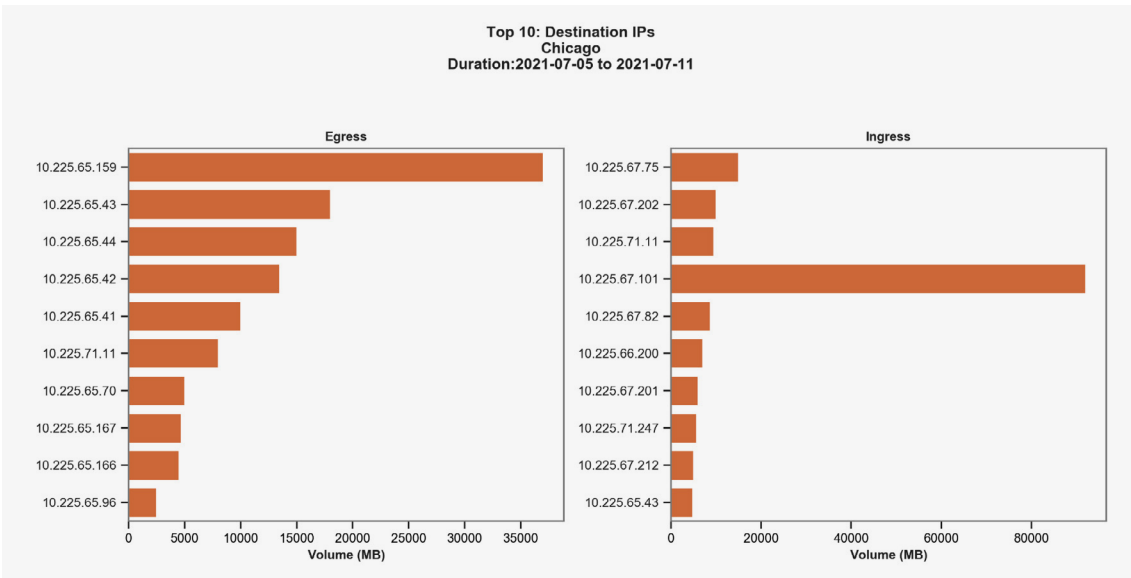


Figure 16: Top 10 Destination IP Report

The report above lists the top 10 destination IP addresses for the Chicago branch for the same duration as analyzed in the **Hotspots Destination IPs Report** in the earlier section. Notice there are some overlapping IP addresses between the two reports, which could prompt an administrator to create one or more custom applications to track performance and utilization for these highly utilized destination IP addresses.

Top N: Undefined Domains Report

The **Top N: Undefined Domains Report** lists the top HTTP and SSL domains that are accessed per site during the week. These domains currently do not map to any system or previously defined custom application signature and may not be appropriately serviced. Instead, these domains will be observed inflows that match the generic application signatures of enterprise-SSL, enterprise-HTTP, HTTP, or SSL. This report helps identify missing domains for existing custom applications or indicates a need to create new custom applications.

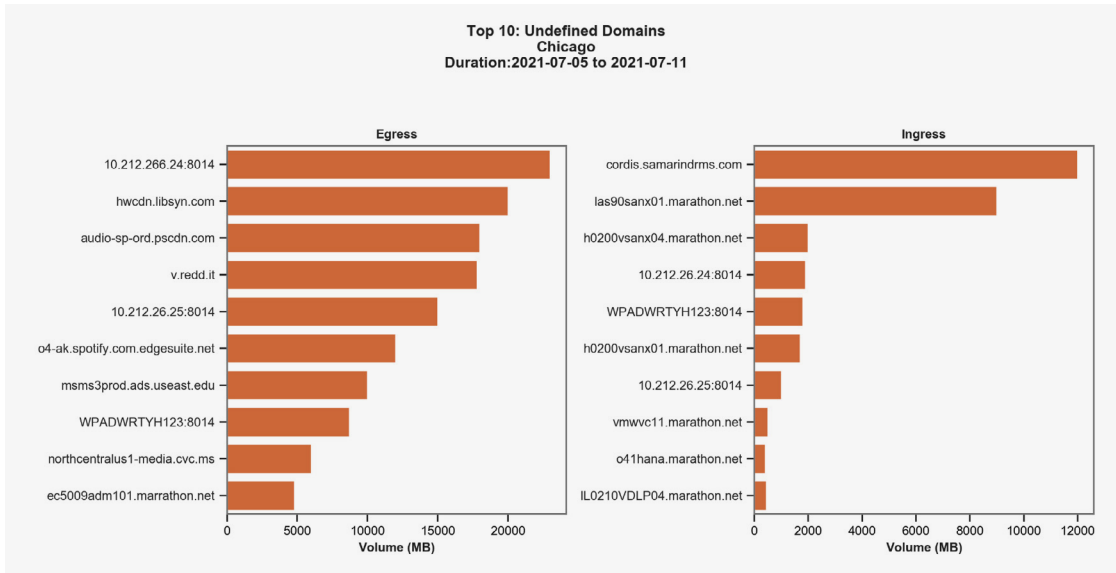


Figure 17: Top 10 Undefined Domains Report

The image above lists the top 10 domains at the Chicago branch. If significant traffic to 10.212.26.24 is observed week after week, an administrator should assess if this domain belongs to an existing application. If not, it is recommended that a custom application be created for this domain to appropriate tracking and policy treatment.

Top N: Source IP Report

The **Top N: Source IP Report** lists the top source IPs for the entire week and is not limited to hotspots. This report is generated per site, unlike the Hotspots Source IP Report, which is specific to periods of hotspots (utilization over 70%) on a particular circuit.

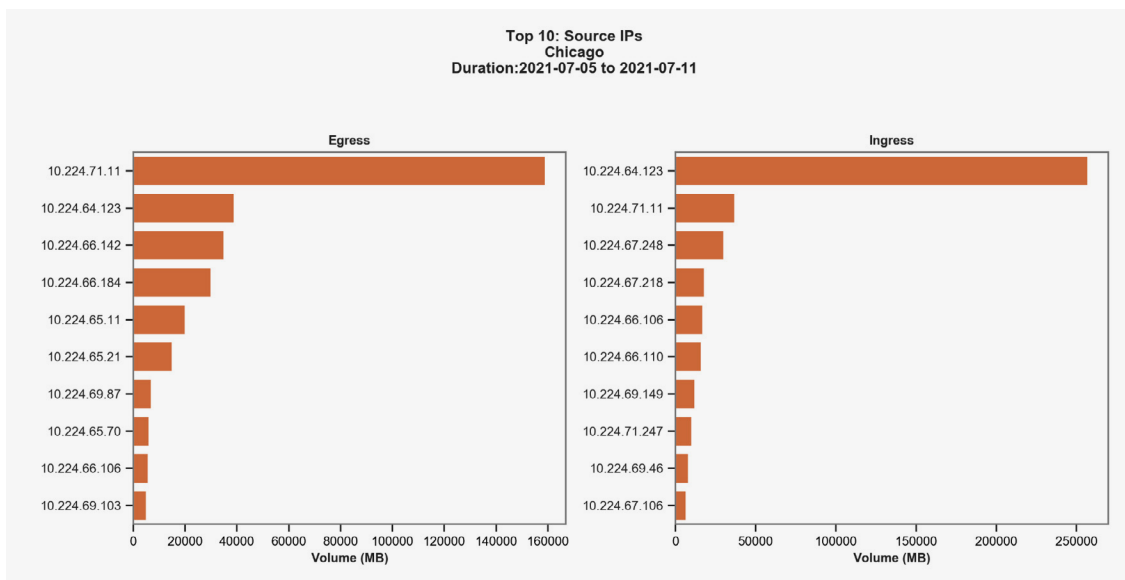


Figure 18: Top 10 Source IP Report

The report above was generated for Chicago for the same duration as the Hotspots Source IP Report, as shown in an earlier section. Note that top users for the week vary from the top users during hotspots. Suppose there is an overlap with the Hotspots Source IP Report. In that case, a possible conclusion could be that the end user experience was impacted, which could have affected Application SLAs.

Top N: Source IP–Destination IP Pairs Report

The **Top N: Source IP–Destination IP Pairs Report** is generated for the entire duration of the week and is not limited to hotspots. This report helps understand traffic flow patterns and consumption trends between source and destination IP pairs.

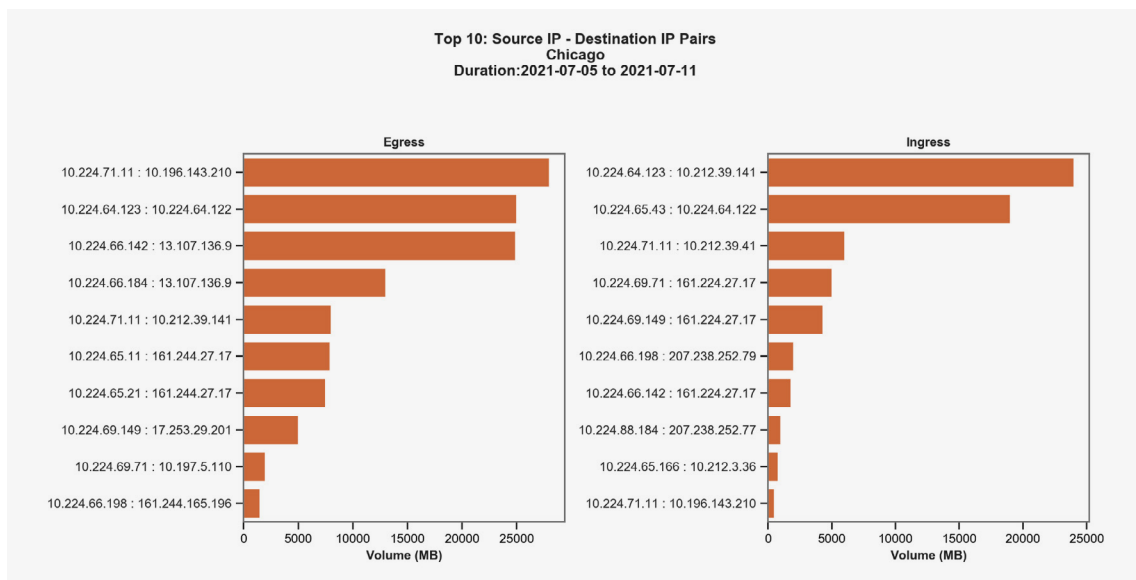


Figure 19: Top 10 Source IP–Destination IP Pairs Report

The report above lists the top source IP–destination IP pairs for the Chicago branch for the same duration as analyzed in the **Hotspots: Source IP–Destination IP Pairs Report** in the earlier section.

Application Volume per Circuit Report

This report lists the total volume of application data transferred per circuit and is provided in a CSV file format. This report helps understand how traffic is shaped and how application traffic is balanced across different available paths. In addition, this data helps redefine path policy. A critical use case is studying application data on metered links. If applications other than mission-critical applications are visible on these links, they can cause unnecessary tariffs on these metered links. An application policy for these links can be rewritten to remove metered links as a possible option in such an event.

Data Center Reports

The Data Center Reports provide an insight into utilization trends from a data center’s perspective. Similar to the branch reports, these reports identify top applications, source IPs, destination IPs, source–destination IP pairs, and undefined domains along with top branches. These sets of reports are also generated for hotspots observed in the data center.

It’s important to note that a hotspot definition for a data center differs from that of a branch. While for branches, utilization over 70% of configured bandwidth was considered a hotspot, 90th percentile utilization is regarded as a hotspot for a data center. It, therefore, becomes imperative that we accurately set the circuit bandwidth allocations at the data center.

It’s essential to understand that these reports approximate **the utilization** trends as the reports generated only consider **overlays paths**.

Traffic Distribution Report

The Traffic Distribution Report helps administrators understand the distribution of traffic volume to all the data centers in the application layer. These reports are provided in Sankey charts that help understand traffic flow from branches, applications, and top applications from top branches to and from the data centers.

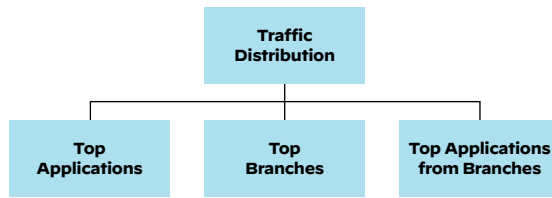


Figure 20: Traffic Distribution Report

These reports are delivered in an HTML report with Sankey charts for the top 10 contenders and a CSV file with the entire dataset.

Traffic Distribution: Top Applications Report

This report details the flow of application traffic to and from all the data centers in the application layer. It provides visibility into the top 10 ingress applications by volume.

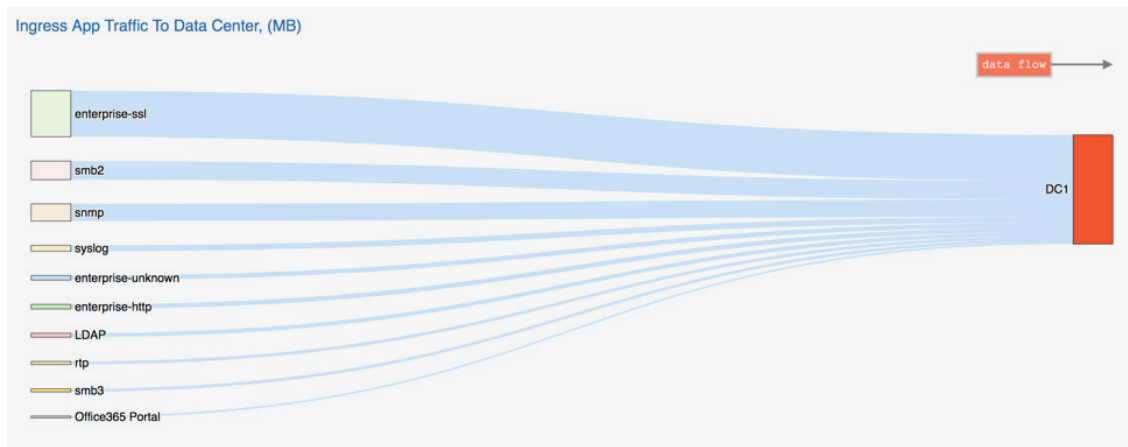


Figure 21: Top Applications Report

The HTML report also provides an insight into top applications by total volume across all the data centers in the form of a combined egress and ingress traffic report.

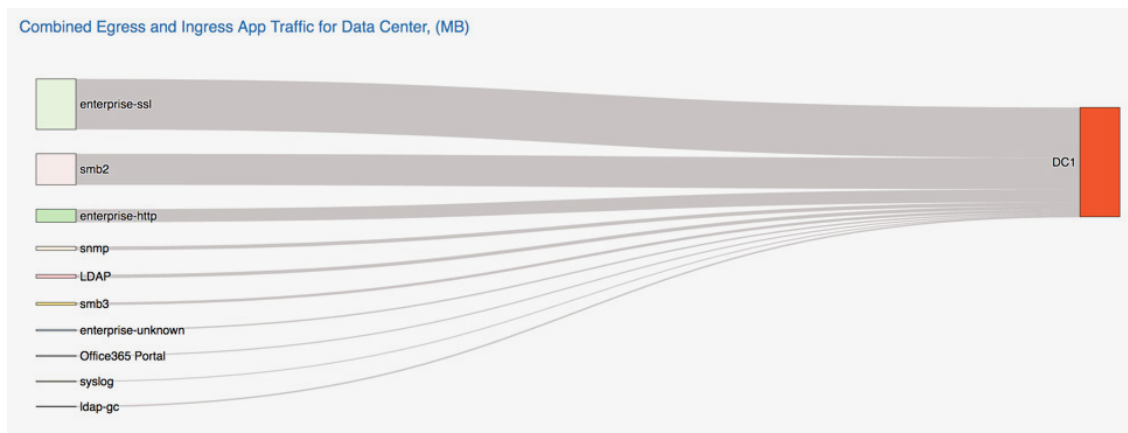


Figure 22: Combined Egress and Ingress Traffic Report

In the examples above, there's only a single data center: DC1. The data flow label above the data center block indicates traffic flow, either to or from that data center.

In the case of multiple data centers, the traffic volume going to each of the data centers can be deciphered from the thickness of the flow stream. The supplemental CSV can help understand the accurate distribution of application traffic volume across the data centers.

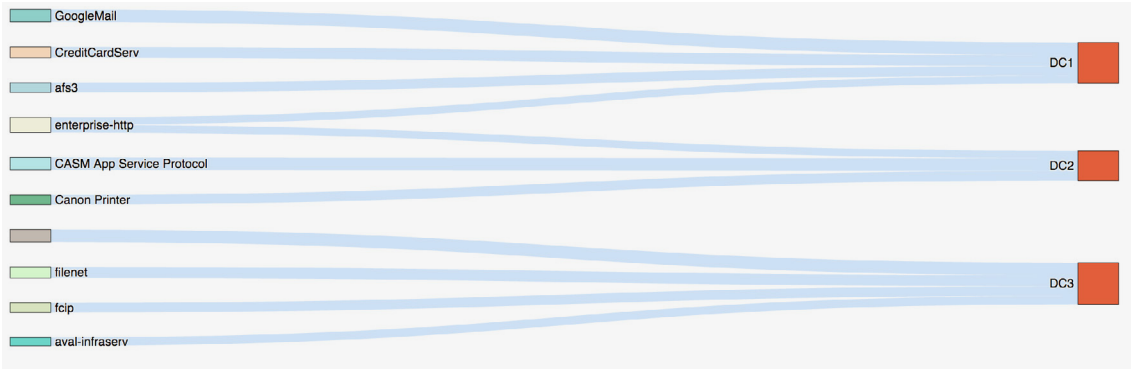


Figure 23: Traffic Volume Report

See the sample report below:

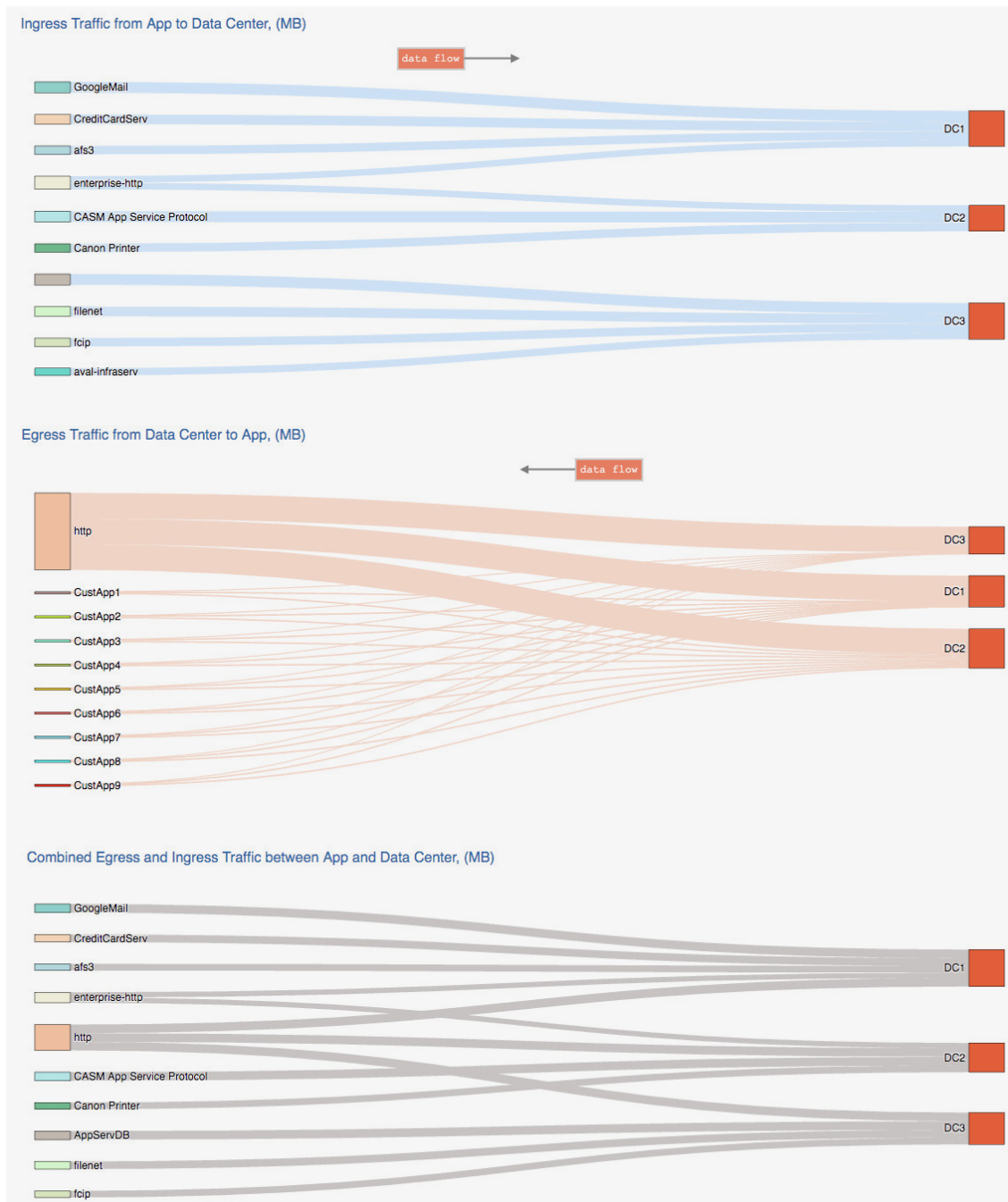


Figure 24: Ingress and Egress Traffic Report

Traffic Distribution: Top Branches Report

Like the Traffic Distribution: Top Applications Report, the Top Branches Report provides details into the flow of branch traffic to all the data centers in the application layer. It provides visibility into the top 10 ingress and egress flows from branches by volume and a combined summary report as well.

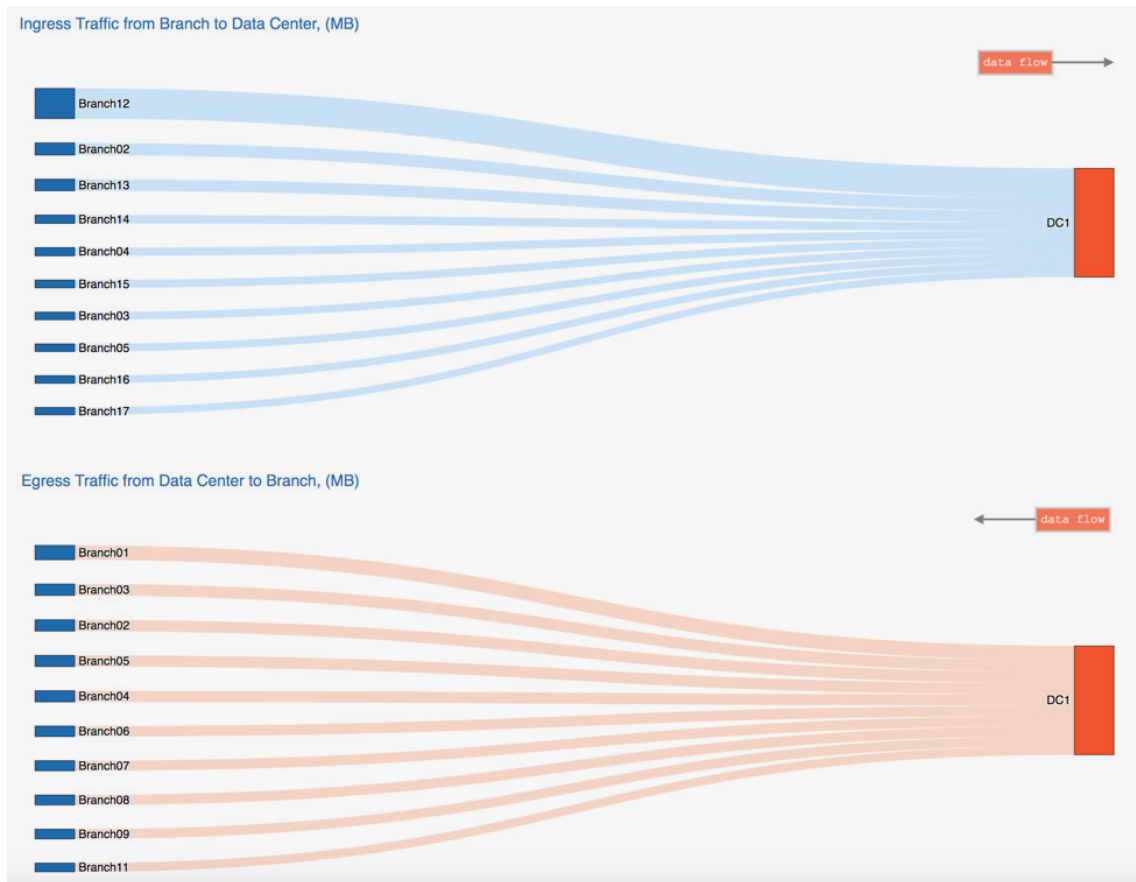


Figure 25: Ingress Top Branches Report

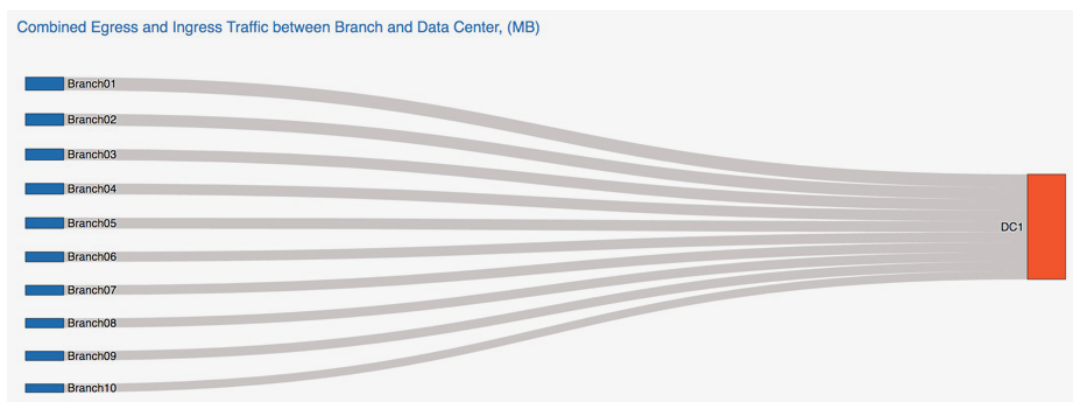


Figure 26: Ingress and Egress Branch Traffic Report

Traffic Distribution: Top Applications from Top Branches Report

This report provides details into the top 10 applications emerging from the top 10 branches to all the data centers in the application layer. The report provides visibility into top ingress and egress branches and the top applications flow by volume emerging from these branches.

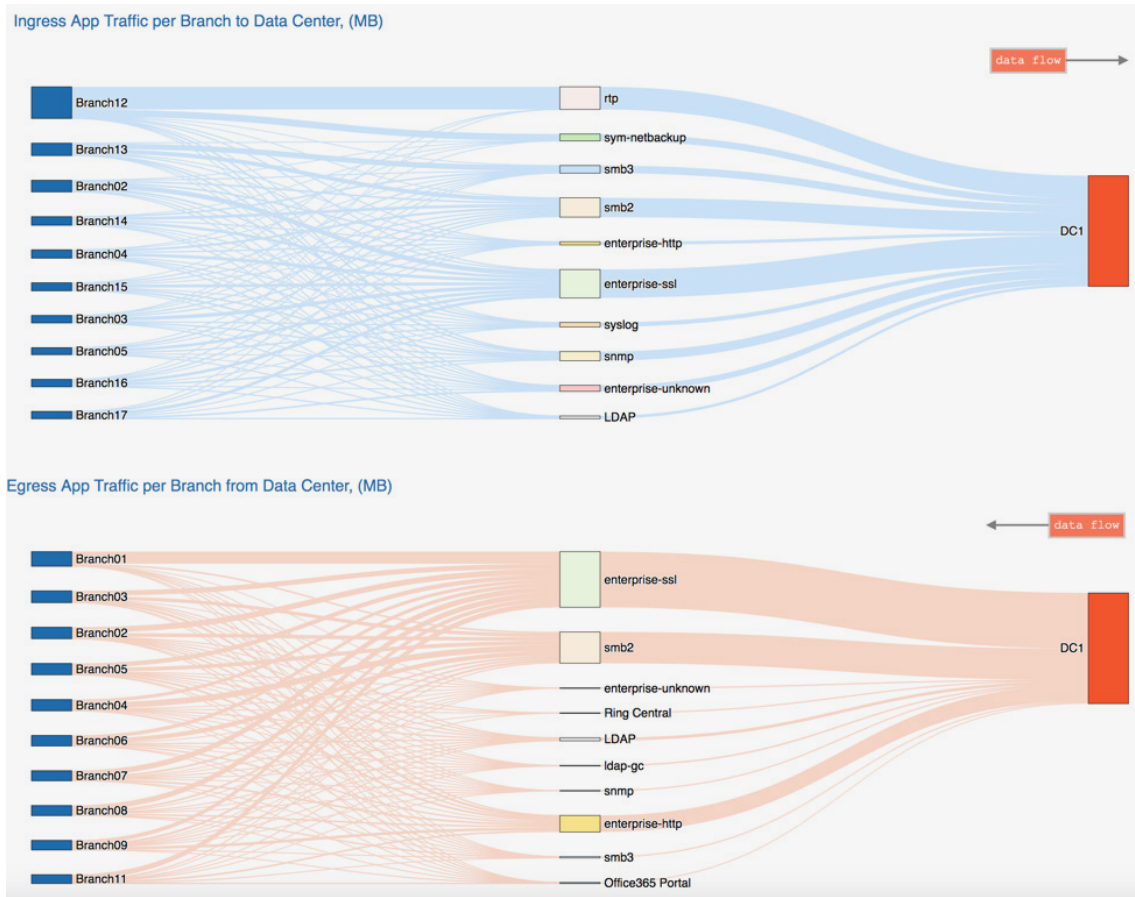


Figure 27: Ingress and Egress Branch to Data Center Traffic Report

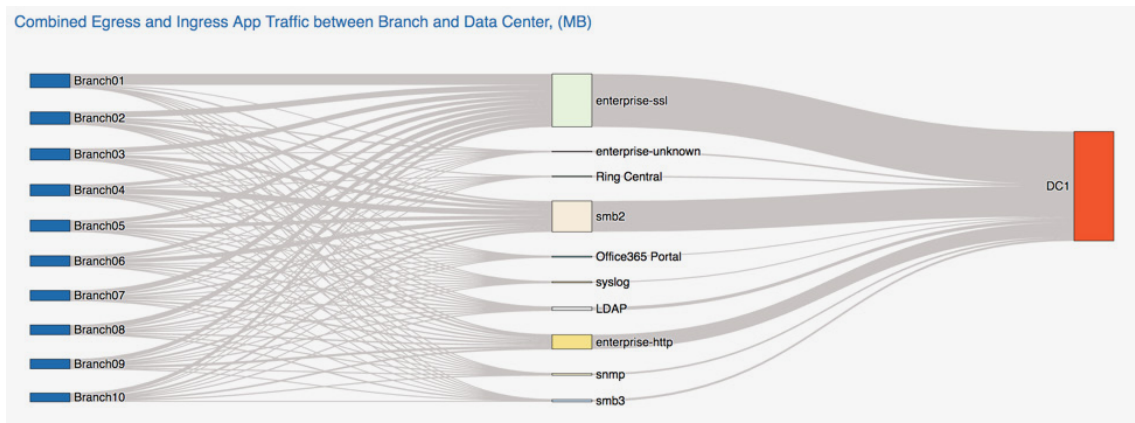


Figure 28: Combined Ingress and Egress Branch to Data Center Traffic Report

Circuit Utilization Report

The Circuit Utilization Report provides a utilization summary for all data center circuits in both the ingress and egress directions. The Circuit Utilization Report consists of raw data packaged in the form of CSV files that have information on **circuit utilization** data and **percentile utilization**. The report package also contains an HTML report for each data center circuit.

The HTML report contains a series of topics that shed light on bandwidth utilization, observed hotspots, branches, applications, source IPs, destination IPs, and unknown domains contributing to those hotspots. We classify a circuit to be hot when the utilization is at the 90th percentile.

The Circuit Utilization Report summarizes the circuit configuration and bandwidth utilization in the form of provisioned bandwidth, median utilization, and 90th percentile utilization.

Attribute	Value
Provisioned Ingress BW	1000.0 Mbps
Median Ingress Utilization	20.02816 Mbps
Median Ingress Percentage	2.00282 %
90th Percentile Ingress Utilization	53.35951 Mbps
90th Percentile Ingress Percentage	5.33595 %

Figure 29: Circuit Utilization Report

The table above is from a report for DC1 - Circuit, where the 90th percentile utilization is at 5.33595% of the provisioned bandwidth, indicating that the circuit is not contentious and possibly overprovisioned.

The Circuit Utilization Report then plots the utilization trend for the past week in an interactive chart that can zoom in and study the trend in detail. It also marks the 90th percentile utilization and highlights hotspots in red.

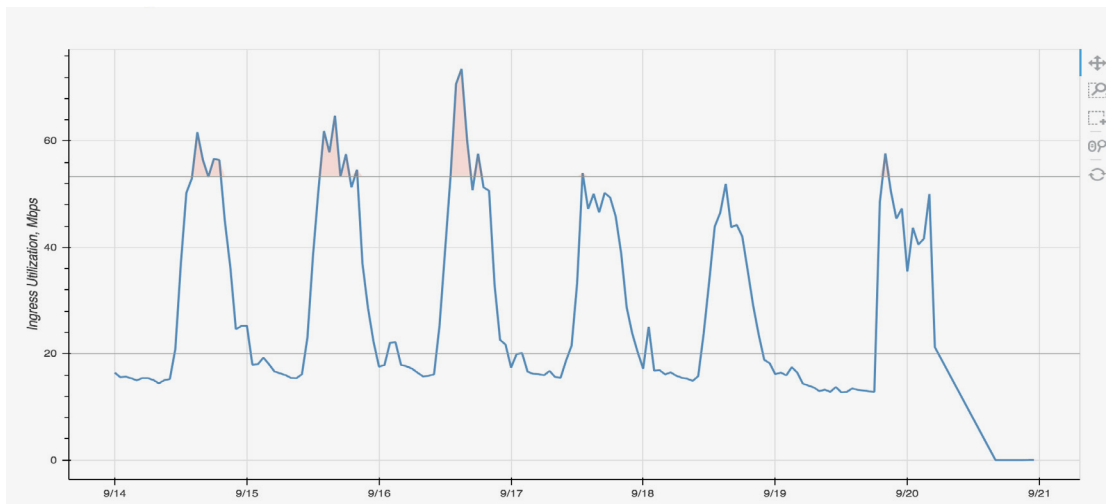


Figure 30: Circuit Ingress Utilization Report

In the sample report above, the utilization above 53.35951Mbps, as mentioned in the table, is highlighted in red as possible hotspots.

The Circuit Utilization Report then highlights the top branches, applications, source IPs (branch IPs for ingress reports), destination IPs (branch IPs for egress reports), IP pairs, and undefined domains contributing to the hotspot. The sample reports below highlight the top contributors to the hotspots for DC1 - Circuit 1.

Hotspot Reports

The **Hotspot Reports** are produced for every circuit at every data center site. A hotspot report for data center circuits gives us visibility into the circuit's 90th percentile utilization. The reports provide a list of branches, applications, undefined domains, destination IPs, source IPs, and source and destination IP pairs observed during the hotspots.

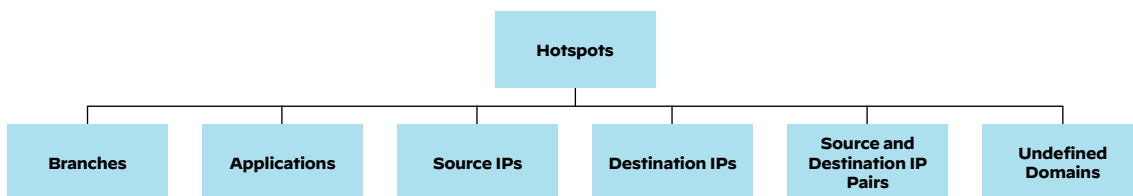


Figure 31: Hotspot Report

The **Hotspot: Top Branches Report** highlights the traffic volume contributed by the top 10 branches during the hotspot observed on the data center circuit.

Top branch transmitting traffic on this circuit when utilization is above the 90th percentile.

Top Branches	Branch Volume (MB)
Branch12	16690
Branch23	9013
Branch27	4961
Branch28	4495
Branch17	4360
Branch16	3863
Branch18	3815
Branch03	3622
Branch29	3600
Branch02	3456

Figure 32: Ingress Hotspot: Top Branches Report

Data from this report can be used to redefine data center transit features under path policies for branches.

The **Hotspot: Top Apps Report** highlights the top 10 applications contributing to the hotspot observed on the data center circuit over the course of the week.

Top applications receiving traffic on this circuit when utilization is above the 90th percentile.

Top Apps	App Volume (MB)
enterprise-ssl	141355
smb2	45970
snmp	29003
enterprise-unknown	21060
smb3	17160
rtp	15392
LDAP	10964
enterprise-http	10480
Ring Central	10296
syslog	10271

Figure 33: Ingress Hotspot: Top Apps Report

Data from this report can be used to redefine path policies for applications that can be directly offloaded to the internet. This report can also help network administrators redefine application priority so that the proper QoS is applied to frequently used applications.

The **Hotspot: Top Undefined Domains Report** highlights the top 10 undefined and defined domains contributing to the hotspot observed on the data center circuit over the week.

Top undefined domains discovered for apps http, ssl, enterprise-http, and enterprise-ssl, receiving traffic on this circuit when

Top Undefined Domains	Undefined Domain Volume (MB)
UnknownDomain-08	20598
UnknownDomain-13	13860
UnknownDomain-15	7851
UnknownDomain-12	7376
UnknownDomain-02	7132
UnknownDomain-05	6900
UnknownDomain-11	5374
UnknownDomain-01	4806
UnknownDomain-14	4177
UnknownDomain-16	3272

Figure 34: Ingress Hotspot: Top Undefined Domains Report

The data from this report can be used to redefine existing custom applications or create new custom applications.

The **Hotspot: Top Source IPs Report** highlights the top 10 source IPs contributing to the hotspot observed on the data center circuit over the week. For the Ingress direction, these IPs are the branch IPs.

Top branch IPs transmitting traffic on this circuit when utilization is above the 90th percentile.

Top Branch IPs	Branch	Branch IP Volume (MB)
10.3.192.194	Branch12	15383
10.191.168.255	Branch23	8352
10.176.122.101	Branch27	2382
10.179.218.195	Branch29	1922
10.181.202.9	Branch30	1350
10.182.163.215	Branch31	1203
10.184.187.114	Branch32	1159
10.177.33.155	Branch33	1128
10.181.75.136	Branch34	1039
10.183.147.218	Branch35	1035

Figure 35: Ingress Hotspot: Top Branch IPs Report

For the egress direction, these IPs will be identified as source IPs (i.e., indicating the origin is the data center).

Top Source IPs transmitting traffic on this circuit when utilization is above the 90th percentile.

Top Source IPs	Source IP Volume (MB)
10.20.206.14	262947
10.20.206.13	170218
10.20.206.15	168317
10.20.206.17	155524
10.20.206.12	152563
10.20.206.16	135183
10.19.150.151	127679
10.20.206.11	83100
10.20.206.26	79602
10.20.203.121	42585

Figure 36: Egress Hotspot: Top Source IPs Report

Data from this report can be used to identify top contributors to the hotspot on the data center circuit and establish proper enforcement of network resources.

The **Hotspot: Top Destination IPs Report** highlights the top 10 destination IPs contributing to the hotspot observed on the data center circuit over the week. For the egress direction, these IPs are the branch IPs, indicating the flow termination is branches in the application level.

Top Destination IPs receiving traffic on this circuit when utilization is above the 90th percentile.

Top Destination IPs	Destination IP Volume (MB)
10.19.150.151	31861
UnknownDomain-15	30538
172.22.16.12	15279
10.20.206.24	13861
172.16.100.100	10149
10.175.197.50	8175
10.240.66.76	7222
10.20.206.13	7210
10.20.21.20	7019
10.240.78.78	7003

Figure 37: Ingress Hotspot: Top Destination IPs Report

Top branch IPs receiving traffic on this circuit when utilization is above the 90th percentile.

Top Branch IPs	Branch	Branch IP Volume (MB)
10.182.114.9	Branch08	8669
10.182.91.164	Branch20	7982
10.180.59.240	Branch25	7651
10.184.75.222	Branch18	7526
10.181.225.253	Branch21	7395
10.185.83.175	Branch03	7116
10.181.147.95	Branch22	6922
10.185.80.16	Branch03	6634
10.183.11.208	Branch09	6346
10.191.171.163	Branch23	6303

Figure 38: Egress Hotspot: Top Branch IPs Report

Data from this report can be used to identify top contributors to the hotspot on the data center circuit and establish proper enforcement of network resources.

The **Hotspot: Top IP Pairs Report** highlights the top 10 source and destination IP pairs contributing to the hotspot observed on the data center circuit over the week.

Top branch (transmitting) and non-branch (receiving) IPs on this circuit when utilization is above the 90th percentile.

Top IP Pair Branch IPs	Top IP Pair Destination IPs	Top IP Pair Branch	IP Pair Volume (MB)
10.3.192.194	172.22.16.12	Branch12	15279
10.191.168.255	10.175.197.50	Branch23	8175
10.176.122.101	10.20.203.121	Branch27	2297
10.179.218.195	10.184.163.7	Branch29	1891
10.184.187.114	10.181.202.9	Branch32	1136
10.182.163.215	10.181.75.136	Branch31	1133
10.177.33.155	10.176.122.255	Branch33	1102
10.181.75.136	10.182.163.215	Branch34	1024
10.183.147.218	10.183.242.169	Branch35	1009
10.181.202.9	10.184.187.114	Branch30	1007

Figure 39: Ingress Hotspot: Top IP Pairs Report

The Circuit Utilization Report is generated for both ingress and egress directions for each data center circuit. It can assess utilization trends, refine path and QoS policies, and identify users who are misusing network resources, enabling the network administrators to enforce proper use of network resources.

Top N Report

Similar to the branch report, the Data Center report also provides a set of Top N Reports. **Top N Reports** provide insight into the top branches, applications, source IPs, destination IPs, source and destination IP pairs, and undefined domains for the entire week. These reports are generated for each data center in the form of a CSV file with information about all the contributors in that specific category.

Insights from this report can be used to understand site-specific trends and turned into actions such as changing path policies, changing application priorities, and reassessing the provisioned bandwidth for oversubscribed and underutilized circuits.

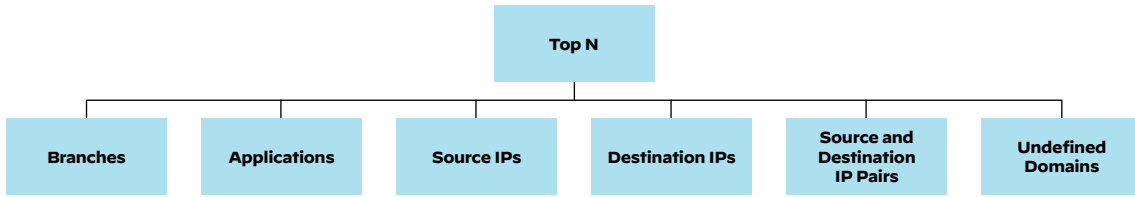


Figure 40: Top N Reports

Unlike the Hotspots Report, which only looks at flows that traversed the network during periods of hotspots, the Top N Report studies flow and application data for the entire week to determine which applications, users, and domains contribute the most to high bandwidth utilization.

Summary

The WAN Clarity Report is generated on a weekly basis to provide administrators a deep understanding of how the circuits in the WAN application layer are being utilized from an entire fabric, site, circuit, application, and user perspective.

These reports provide actionable insights that can be used for:

- Capacity planning
- Path policy adjustments
- QoS policy adjustments
- Enforcement of proper use of network resources by the end user community

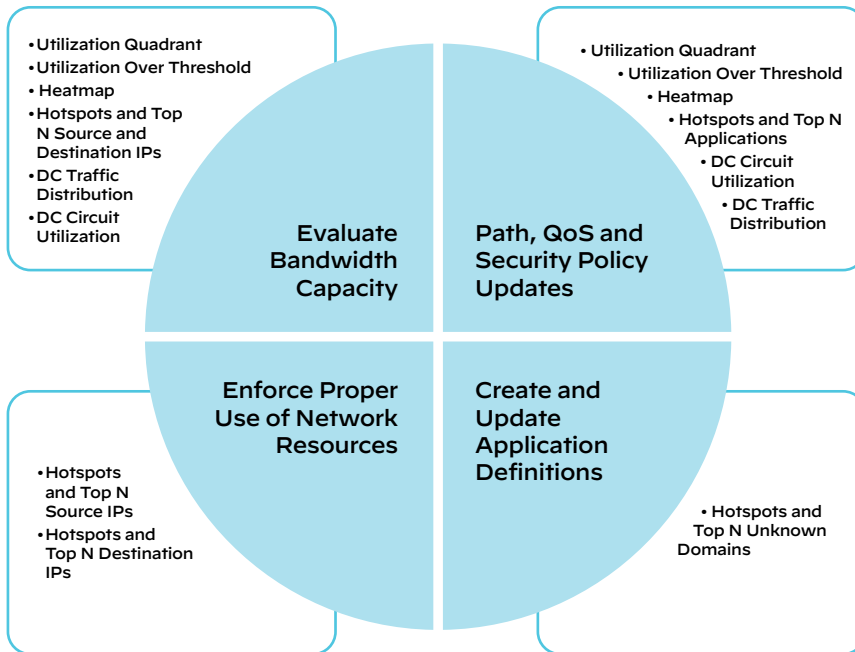


Figure 41: WAN Clarity Report

Circuit Insights/AIOps Insights

Prisma SD-WAN now provides valuable insights powered by AI. These insights are generated after a deep analysis of utilization and application performance trends. Customers can use these insights for capacity planning, and making sure configurations are compliant and in tune per carrier provisioned specifications.

Bandwidth Upgrade Recommendation

The Bandwidth Upgrade Recommendation insight is generated when utilization for a given circuit is observed to be over 90% of the configured bandwidth. This weekly insight is generated only if high utilization is measured on the circuit for at least 10 hours over the entire duration of the week.

The report provides details about the traffic direction, ingress, or egress, where high utilization was observed, a box plot for bandwidth distribution, median latency, and packet loss during the hotspot. It also provides the total duration the circuit was down or running hot, i.e., over 90% of configured bandwidth.

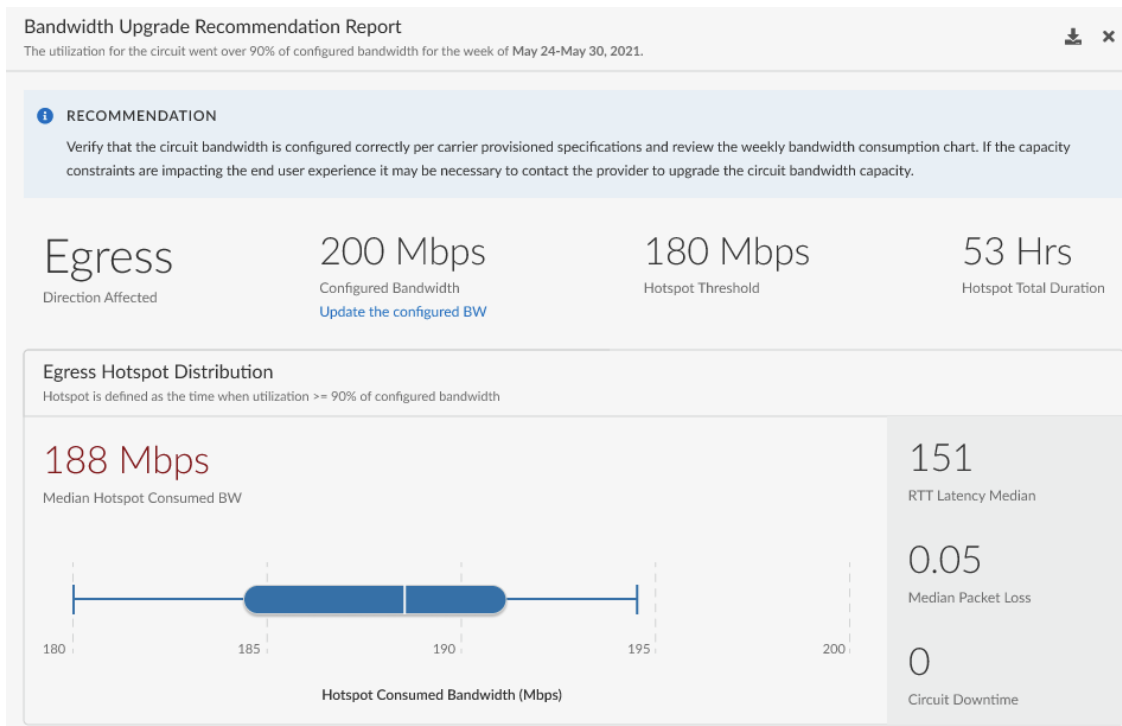


Figure 42: Bandwidth Upgrade Recommendation Report

If this insight is generated for a circuit, customers should closely monitor this circuit and consider upgrading the circuit capacity as the capacity constraints may be impacting the end user experience.

Configured vs. Consumed Bandwidth Mismatch

This weekly insight is generated for circuits where utilization is observed to be over 200% of the configured bandwidth. This weekly insight is generated only if QoS is disabled on the circuit and high utilization is measured on the circuit for at least 10 hours over the entire duration of the week.

Similar to the Bandwidth Upgrade Recommendation insight, this insight also provides details about the traffic direction, ingress or egress, where high utilization was observed, a box plot for bandwidth distribution, median latency and packet loss during the hotspot. It also provides total duration the circuit was down or running hot, i.e., over 200% of configured bandwidth. The confidence for this insight is Excellent when we have PCM measurements corroborating the utilization trend. This confidence score is otherwise set to Good.

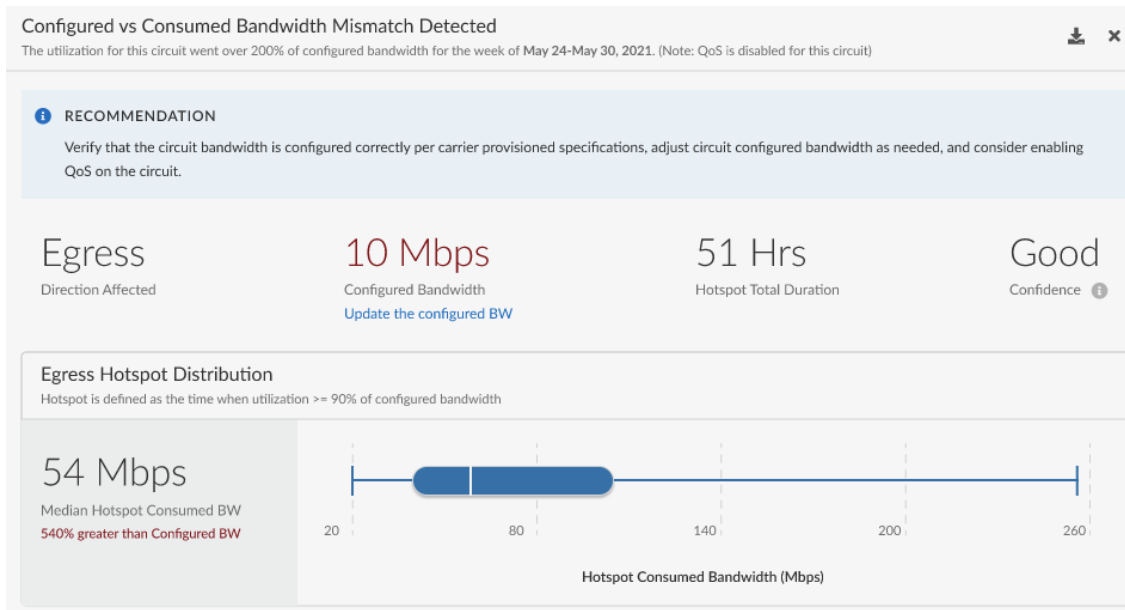


Figure 43: Configured vs. Consumed Bandwidth Mismatch Report

If this insight is generated for a circuit, customers should correctly configure the circuits per carrier-provisioned specifications and also enable QoS to avoid impacting the end user experience.

Excessive Packet Loss

This insight is generated for a rolling three-week period and provides a packet loss profile for that duration. When circuits run at capacity, the contention in the networks results in packet loss. However, network administrators need to investigate if excessive packet loss is observed when the circuit is nowhere near at capacity. The Excessive Packet Loss insight is generated when an abnormal packet loss is observed on the circuit for ingress or egress direction and provides mean and median packet loss measurements for a range of circuit utilization.

Excessive Packet Loss Detected

The circuit experienced abnormal egress packet loss during the 3 week period Mar 01 - Mar 21, 2021.



RECOMMENDATION

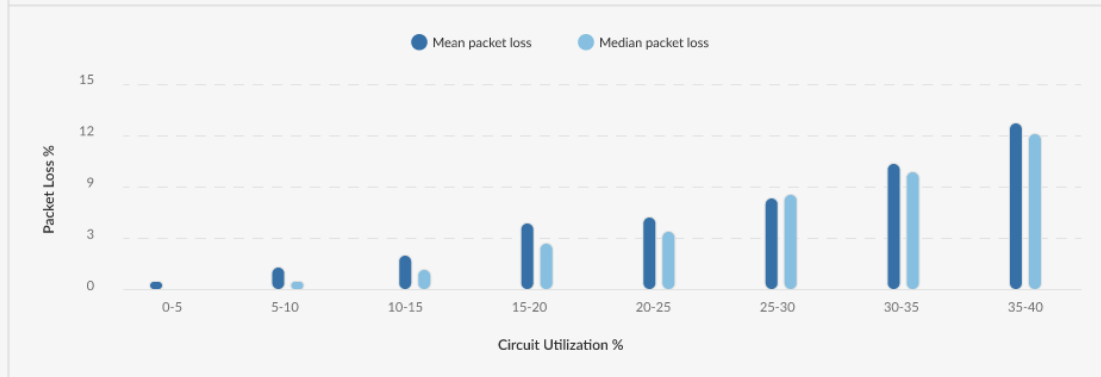
Verify that the circuit bandwidth is configured correctly per carrier provisioned specifications. If these values match then it may be necessary to contact the provider to ensure that the circuit is provisioned and performing as expected.

Egress

Direction Affected

Mean and Median Packet Loss vs Utilization

Shows the mean and median egress packet loss samples for different circuit egress utilization percents



Circuit Utilisation %	Mean Packet Loss %	Median Packet Loss %	Sample Count ↓
0-5	0.23	0	45756
5-10	1.06	0.17	7919
10-15	1.91	1	2175
15-20	3.51	2.83	1418
20-25	4.5	4	1116
25-30	6.96	6	650
30-35	10.24	10.33	775
35-40	12.04	11.17	357

Figure 44: Excessive Packet Loss Report

Customers can use this insight to verify that the circuit bandwidth is configured correctly per carrier-provisioned specifications. Carrier provider intervention may also be needed if the configuration is accurate.

Excessive Latency

This insight is generated for a rolling three-week period and provides a latency profile for that duration. When circuits run at capacity, the contention in the networks results in high latency. However, network administrators need to investigate if excessive latency is observed when the circuit is nowhere near at capacity. The Excessive Latency insight is generated when an abnormal latency is observed on the circuit and provides mean and median latency measurements for a range of circuit utilization.

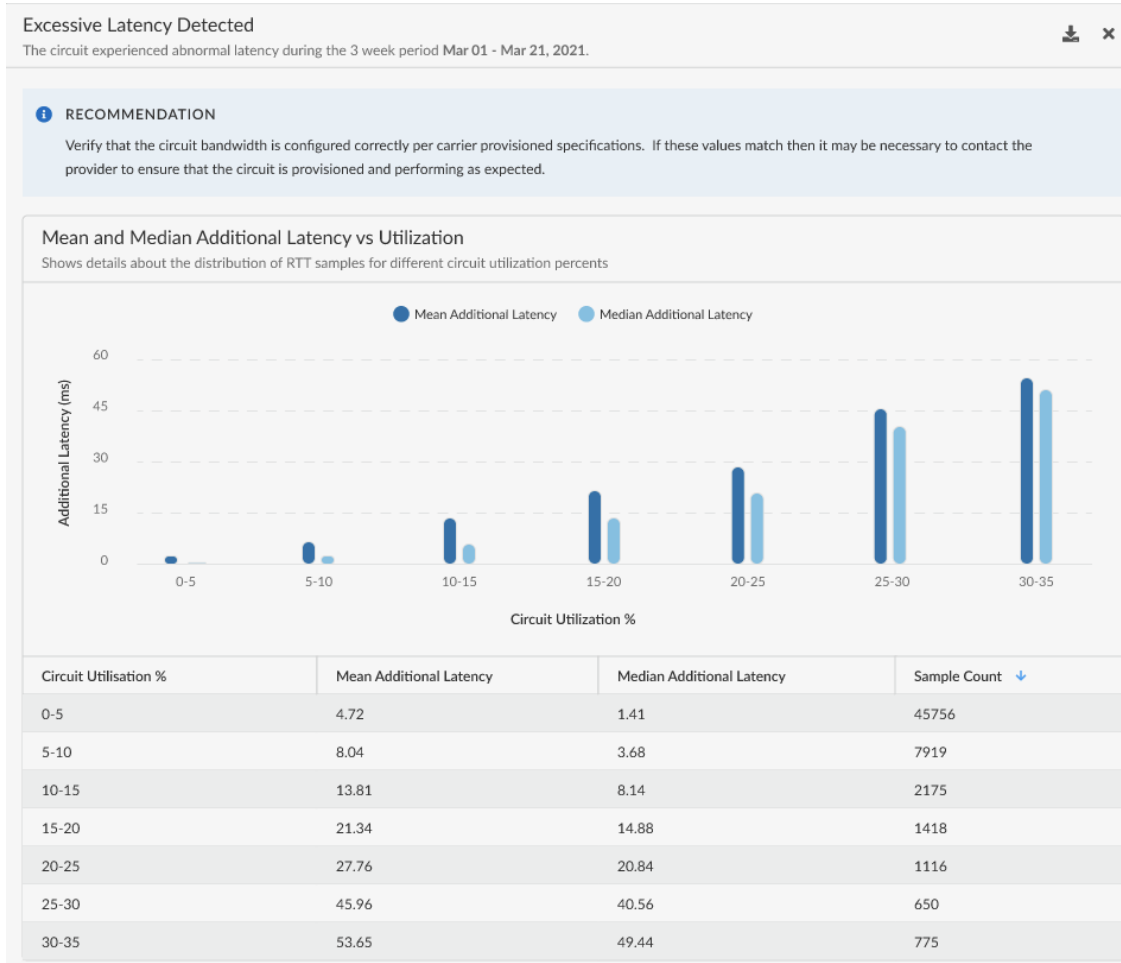


Figure 45: Excessive Latency Report

Customers can use this insight to verify that the circuit bandwidth is configured correctly per carrier-provisioned specifications. Carrier provider intervention may also be needed if the configuration is accurate.

Low Circuit Throughput

This insight is generated for circuits where the observed throughput is lower than the configured circuit capacity. This rolling three-week-period insight is generated only if the observed capacity is at 30% or lower than the configured capacity. To deterministically state the circuit throughput is low, all of the following measurements should indicate low measured throughput:

- Latency profile at the circuit
- 99th percentile for the maximum utilization at the circuit interface
- Maximum throughput received for a bulk transfer
- PCM indicating lower bandwidth measurement

Only if all of the above measurements indicate a lower throughput, the insight is generated for the circuit.

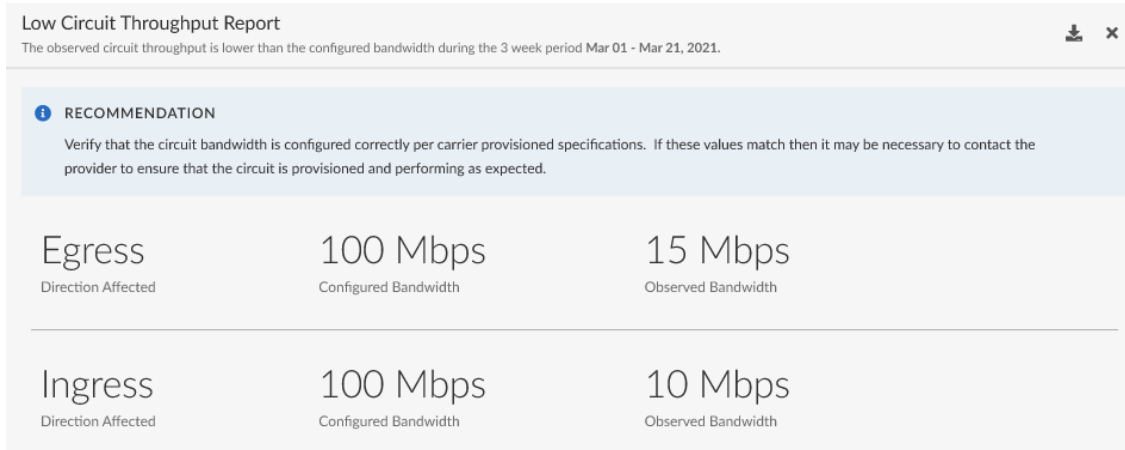


Figure 46: Low Circuit Throughput Report

Customers can use this insight to verify that the circuit bandwidth is configured correctly per carrier-provisioned specifications. Carrier provider intervention may also be needed if the configuration is accurate.