Packet Analyzer Deployment

This chapter describes some usage cases on how to deploy Packet Analyzer in your networks. It contains details on network performance management as well as usage scenarios for the Cisco Security Packet Analyzer Software.

The use cases focus on a specific need to be addressed or a problem to be solved. Each scenario takes into account the deployment considerations discussed in Overview and then uses one or more of Packet Analyzer's features to meet the need or solve the problem. The goal of these use cases is to provide real-world examples. These examples discuss best practices and approaches to effective Packet Analyzer deployment and are grouped into several categories.

This chapter contains the following sections:

Note Some of the graphics represented in this section may be different than what you see on the screen. These illustrations are for examples only.

Deploying in the Data Center

Deploying in a Campus Environment

- Using Packet Analyzer to Evaluate Application-Level Performance Monitoring for UDP Real-Time Applications, page 6-14
- Using Packet Analyzer to Monitor QoS/DiffServ (DSCP), page 6-10
- Using Packet Analyzer to Monitor VoIP Quality, page 6-3

Deploying in the Branch

- Using Packet Analyzer to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications, page 6-14
- Using Packet Analyzer to Evaluate Application-Level Performance Monitoring for UDP Real-Time Applications, page 6-14
- Using Packet Analyzer to Monitor QoS/DiffServ (DSCP), page 6-10
- Monitoring Cisco WAAS and Measuring Its Impact, page 6-6
- Using Packet Analyzer to Monitor VoIP Quality, page 6-3

General Usage Scenarios

These use cases are applicable to any part of the network:

- Using Packet Analyzer for Historical Trends via Interactive Report, page 6-12
- Using Packet Analyzer for Problem Isolation, page 6-15
- Creating Custom Applications, page 6-5
- Auto-Discovery Capabilities of Packet Analyzer, page 6-4
- Using Packet Analyzer for SmartGrid Visibility, page 6-15

Packet Analyzer Integrations with Monitoring and Reporting Applications

- Integrating Packet Analyzer with Prime Infrastructure, page 6-5
- Integrating Packet Analyzer with Third Party Reporting Tools, page 6-6

Deployment Examples

- Using Packet Analyzer to Monitor VoIP Quality, page 6-3
- Auto-Discovery Capabilities of Packet Analyzer, page 6-4
- Creating Custom Applications, page 6-5
- Integrating Packet Analyzer with Prime Infrastructure, page 6-5
- Integrating Packet Analyzer with Third Party Reporting Tools, page 6-6
- Monitoring Cisco WAAS and Measuring Its Impact, page 6-6

Using Packet Analyzer to Monitor VoIP Quality

Voice quality analysis has been significantly enhanced in Packet Analyzer. The software is now capable of accurately measuring voice quality by using the industry-standard MOS algorithm. Call quality measurements are computed every 1 minute and made available through the GUI. Note that the voice-related screens on the Packet Analyzer GUI are significantly different from previous releases. Changes have been made to provide useful information quickly and automatically, while allowing easy navigation to details.

Deployment: Packet Analyzer deployments for voice quality analysis require that Packet Analyzer be able to monitor VoIP packets from the calling phone to the called phone. The branch edge location in the network provides visibility into all calls entering and leaving the branch; similarly a campus edge location monitors calls crossing the campus boundary. Often, the distribution layer is a good location to deploy Packet Analyzer for this purpose, especially if specific phones or particular portions of the network are to be monitored. For example, a new Multi protocol Label Switching (MPLS) link is being piloted and three buildings that are part of Company X's headquarters are part of the pilot. In order to monitor voice quality for those three buildings, a Packet Analyzer could be deployed at the distribution Catalyst 6500 that serves those users.

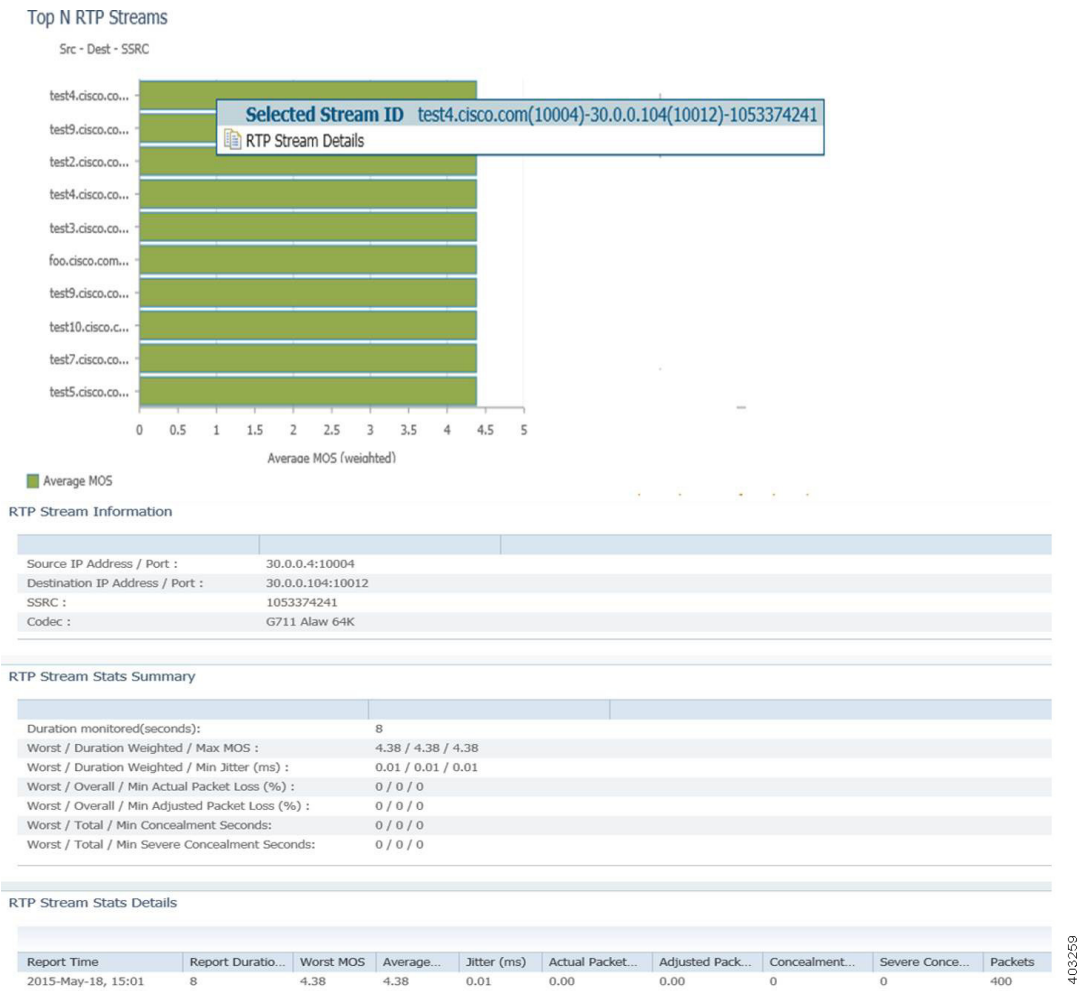
Note The data center is typically not an appropriate location for RTP stream analysis because calls will seldom go through the data center. However, the data center is a good location to monitor signaling messages between phones and Cisco Unified Communications Manager. Packet Analyzer decodes signaling messages to track call history, caller names, phone numbers, and other relevant call details.

Use the following steps to monitor the network to make sure that call quality is good. If quality issues appear, isolate and troubleshoot the problem rapidly.

Step 1 View RTP Streams using the menu selection **Analyze > Media**. This chart indicates current voice quality of all RTP streams being monitored. MOS values range from 1 to 5, where 1 is poor and 5 is excellent (see the legend for a breakdown into categories-Poor, Fair, Good and Excellent). The figure below displays the Top N RTP Source and Destination endpoints. Notice that there are calls that are in the poor range.

Step 2 To isolate calls that had a poor MOS, scroll down to Top N RTP Streams and click on the chart to drill down into the RTP Stream Details. See Figure 6-1.

Figure 6-1 Top N RTP Streams by MOS



Step 3 With the endpoints' IP addresses, you can look at the network topology to identify where in the network the 50.5.10.38 subnet is located. For the purposes of this use case, this subnet is in Building 3 of the main campus. You know that the Building 3 distribution switch has a Packet Analyzer located in it.

Navigate to that Packet Analyzer and go to the menu selection **Analyze > Managed Device > Interface**. This page lists all interfaces and errors or discards on each interface. Look up the link that leaves Building 3 and connects to the core. That interface is likely the source of the packet loss. Check the interface for faults and fix as needed.

See Analyzing Traffic, RTP Streams, page 3-33 and Setting Voice Signaling Thresholds, page 7-37.

Auto-Discovery Capabilities of Packet Analyzer

Auto-discovery data source is enabled by default for ERSPAN, NetFlow, and WAAS data that are sent from remote device to Packet Analyzer management port. Packet Analyzer user has the option to disable any of the three auto-discovery. When auto-discovery is enabled, Packet Analyzer automatically creates ERSPAN data source, NetFlow data source, and/or WAAS data source based on the data type being received at the Packet Analyzer management interface.

Creating Custom Applications

Packet Analyzer identifies applications/protocols based on the TCP/UDP port number, so if there are applications using custom ports, the Packet Analyzer can be configured to identify those applications by name instead of the port.

See Creating Deeper Visibility Into Application Traffic, page 7-56.

Integrating Packet Analyzer with Prime Infrastructure

Cisco Prime supports integrated lifecycle management of networks, services, and endpoints for Cisco borderless network, data center, and collaboration architectures with end-to-end assurance. You can use Cisco Prime Infrastructure to centrally manage the Cisco Packet Analyzer platforms such as the Packet Analyzer appliance to track inventory, view configurations, and perform image and fault management. Prime Infrastructure also rolls up the performance intelligence from Packet Analyzer deployed across the network into a consolidated dashboard.

The following overview describes the steps to complete in Prime Infrastructure to set up Packet Analyzer to view multiple Packet Analyzer on your dashboard. For details steps, see the *Prime Infrastructure User Guide* on Cisco.com.

Step 1 Ensure you configure NTP and DNS for all the Packet Analyzer in your network. You can now configure those without going to the CLI or logging in to the individual Packet Analyzer web GUI. Use the Cisco Prime Infrastructure Device Work Center to perform this task. For detailed steps, see your Prime Infrastructure product documentation.

Step 2 Add the Packet Analyzer HTTPS credentials from the Prime Infrastructure's Device Work Center Edit Device window so that Prime Infrastructure can retrieve data from them. You must add them only after the discovery process is complete or the modules have been added to the Prime Infrastructure inventory.

If you have licensed Assurance features, most Assurance features depend on Packet Analyzer data to work so this is a required step.

You can repeat this task for all Packet Analyzer from which you want Prime Infrastructure to collect data.

Step 3 To ensure that you can collect data from your Packet Analyzer using Prime Assurance, you must enable Packet Analyzer data collection and configure your NetFlow-enabled switches, routers, and other devices (ISR/ASR) to export this data to Prime Infrastructure. You can do this for each discovered or added Packet Analyzer, or for all Packet Analyzer at the same time.

Step 4 To manage and troubleshoot a network problem such as a suspected network attack, you can use multiple Packet Analyzer to create packet captures, save them as files, and then decode them to inspect the suspicious traffic.

For other troubleshooting tips on how to use Packet Analyzer with Prime Infrastructure, see the *Prime Infrastructure User Guide.* For application developers who want to use the Packet Analyzer REST API to connect with Packet Analyzer, ask your Cisco representative about using the Cisco Security Packet Analyzer REST API.

Integrating Packet Analyzer with Third Party Reporting Tools

Packet Analyzer integrates with the CA NetQoS SuperAgent for the purpose of aggregating Application Response Times. Packet Analyzer also integrates with CompuWare Vantage and InfoVista 5View for Host, Conversation, RTP, and Response Time.

Ask your Cisco representative about the *Cisco Security Packet Analyzer API Programmer's Guide* to find out more about the Packet Analyzer Northbound Interface, also referred to as the REST API (Application Programming Interface). The API enables you to provision Packet Analyzer and extract performance data.

You can write your own scripts based on the Packet Analyzer Northbound API, but you must perform some setup in the GUI.

For details on what data can be collected, see Using Response Time Summary.

Monitoring Cisco WAAS and Measuring Its Impact

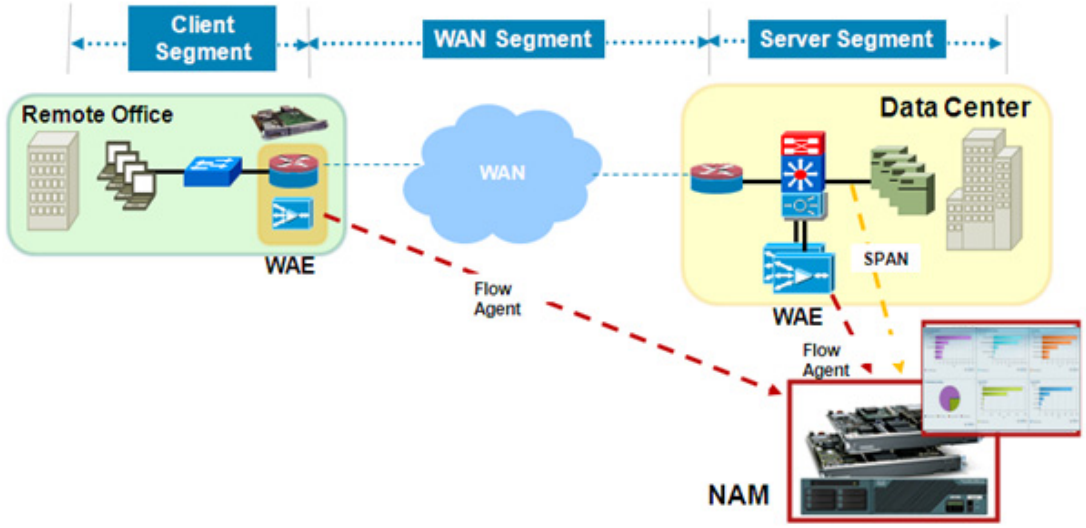
Cisco Wide Area Application Services (WAAS) is a comprehensive WAN optimization solution that accelerates applications over the WAN, delivers video to the branch office, and provides local hosting of branch-office IT services. Cisco WAAS allows IT departments to centralize applications and storage in the data center while maintaining LAN-like application performance and provides locally hosted IT services while reducing the branch-office device footprint.

One of the challenges facing IT personnel who deploy WAAS is to measure and report on the benefits provided by their WAN optimization deployment. Accurate measurement provides many benefits: IT can show return on investment; IT can assess whether the improvement gained meets originally advertised expectations from the solution; and finally, IT can use WAAS ongoing for monitoring, troubleshooting, and planning information for expanding the deployment.

The Packet Analyzer can monitor WAAS-optimized flows by using WAE devices as the data source. Using this capability, the Packet Analyzer is able to provide visibility into optimization-related metrics for the three distinct segments that are created by WAAS: the branch, the WAN, and the data center segments.

Placing a Cisco Packet Analyzer appliance at the edge of the data center is recommended for WAAS deployments. From this location in the network, the Packet Analyzer can measure local metrics using SPAN technology, and for information on the remote branch segment, it relies on flow agent exports from the remote WAE device. See Figure 6-2.

Figure 6-2 Cisco Packet Analyzer's Ability to Analyze from Multiple Data Sources



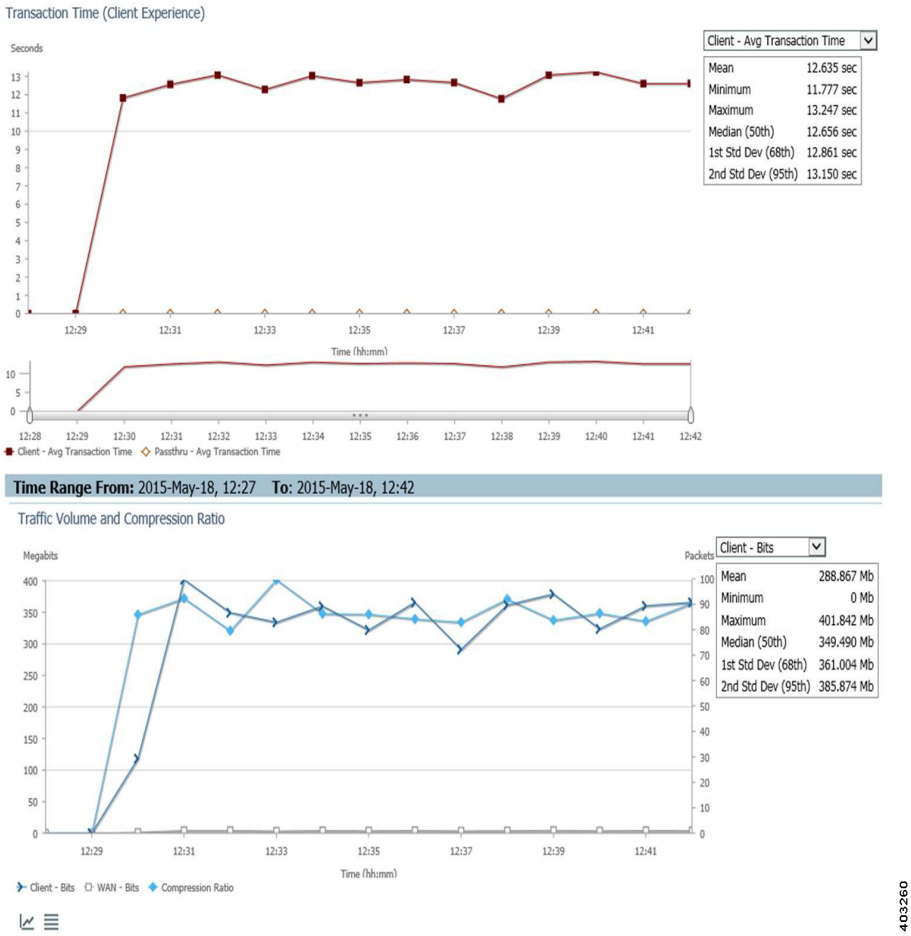
To deploy this solution:

Step 1 Using a Packet Analyzer 2x20 deployed at the data center, measure application response time before WAAS is enabled using **Analyze > WAN Optimization > Top Talker Detail**. The Top Talker display includes such data as utilization, concurrent connections, and average transaction time for top applications, network links, clients, and servers that are possible candidates for optimization.

Step 2 Create a WAAS Client Side and WAAS Server Side for the WAAS flows from the DC and Branch WAEs.

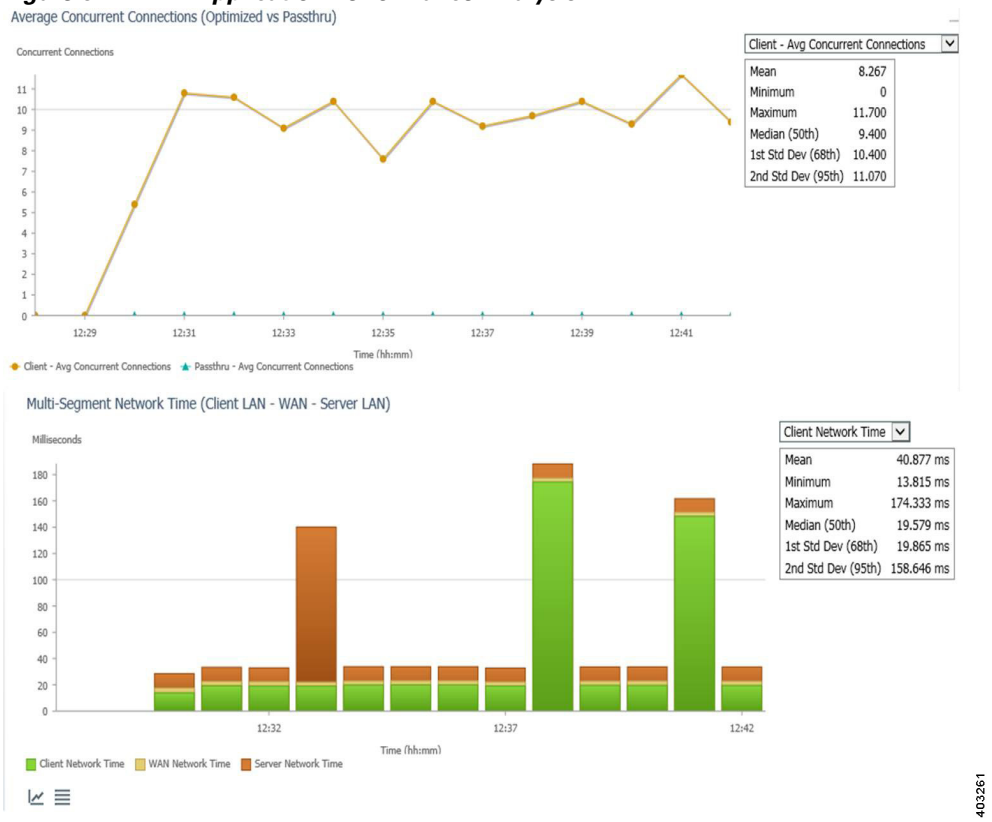
Step 3 The Packet Analyzer provides an interactive dashboard to view the analyzed data. Figure 6-3 displays Client Transaction Time, Traffic Volume and Compression Ratio, Number of Concurrent Connections (Optimized vs. Passthru), and Multi-Segment Network Time (Client LAN - WAN - Server LAN). As you can see in the first graph, all non-optimized traffic is displayed as Passthru.

Figure 6-3 Application Performance Analysis -- Optimized



The screen shot above illustrates the significant improvement experienced by users in the branch when WAAS is turned on. Such reports are very useful to justify an investment in WAN optimization technologies and to show returns on those investments in terms of increase in employee productivity and improved user experience from remote sites.

Figure 6-4 Application Performance Analysis



Step 4 From the perspective of the Packet Analyzer located in the data center, there are two sources of information for response time measurements. SPAN provides measurement at the data center and exports from the branch; WAAS flow or PA via Prime Infrastructure provides measurements from the branch. Using these two sources of information, the Packet Analyzer at the data center can continuously monitor current response times for each branch and help IT personnel keep user experience within known bounds. When abnormal response times are detected, the Packet Analyzer can be configured to send alerts to appropriate personnel with information relevant to troubleshooting the problem.

Monitoring

Using Packet Analyzer to Monitor QoS/DiffServ (DSCP)

Differentiated Services (DiffServ) provides insight into how traffic is being classified by QoS and detects incorrectly marked or unauthorized traffic. The Packet Analyzer identifies the application/protocol based on the type of service (ToS) bits setting. The administrator can configure DSCP Groups or use the ones provided. The voice template can be used to monitor whether voice traffic is marked properly. Figure 6-6 displays the DiffServ application statistics for all DSCP value. Looking at this, you will notice that RTP and Session Initiation Protocol (SIP) are listed, which indicates that they are not being correctly marked throughout its path.

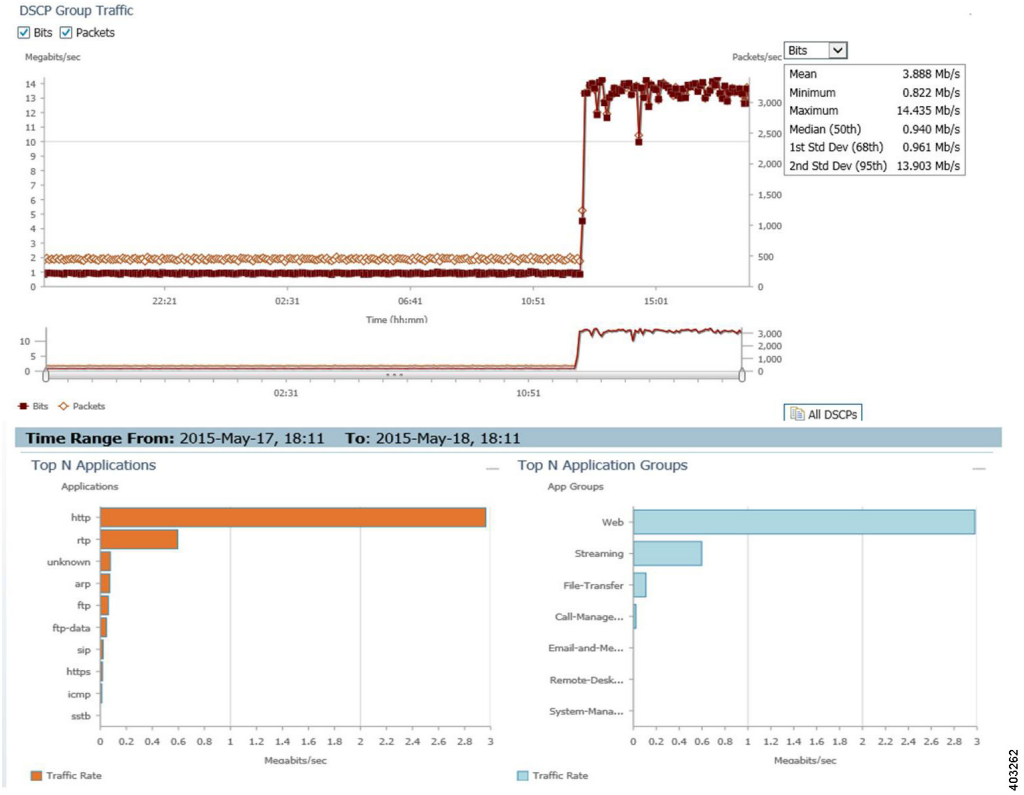
In the following scenario, IT has deployed QoS to prioritize VoIP traffic to improve voice quality across the network. The Packet Analyzer are deployed in the data center and branches and utilized to monitor the DSCP to validate QoS policies.

Step 1 Choose **Setup > Network > DSCP Groups** to display the default groups.

Step 2 Choose **Administration > System > Preferences** to turn the IP TOS Flow Key on. Use caution since this option affects ART and other flow-based traffic. See Table D-71 for details.

Step 3 Choose **Analyze > Traffic > DSCP** to find any misclassified traffic. In Figure 6-5, the RTP protocol is displayed for ToS0 classification.

Figure 6-5 DSCP Group - ToS0



Step 4 Click on the **All DSCP** button to view all DSCP and applications.

Step 5 In Figure 6-6, RTP and SIP are highlighted. The protocols are listed for DSCP 0, which is incorrect since the standard classification for voice traffic is DSCP 46 and 24. This means that some of the voice traffic is misclassified on the network. You can also view the branch Packet Analyzer to investigate whether voice traffic is being misclassified.

Figure 6-6 All DSCP Table

DSCP	Application	Bits/sec	Packets/sec
0	http	12,505,501.99	2,661.51
0	rtp	596,727.20	137.11
0	ftp	84,646.97	160.12
0	unknown	77,680.74	41.29
0	arp	71,747.56	131.89
0	ftp-data	45,533.71	22.26
0	sip	22,247.05	7.22
0	https	16,748.38	2.95
48	icmp	10,999.32	4.09
0	wbem	7,566.72	1.20
0	sstb	5,993.60	10.43
0	nntp	3,836.32	1.86
48	igmp	893.37	1.64
0	snmp	813.27	1
0	rtsp	278.65	0.23
0	stp-l2	256	0.50

Step 6 Left-click on the RTP graph and select **Application Traffic by Host** to display the clients using those protocols. This helps to troubleshoot why RTP or SIP traffic from these clients is not marked correctly. As shown in Figure 6-7, the Packet Analyzer displays the IP addresses of the phones using those protocols. This helps you review the QoS policy implemented on the routers and switches between the clients.

Figure 6-7 RTP Host Table

Analyze > Traffic > Detailed Views > **Application Traffic By Hosts**

Interactive Report

Filter

Site **Unassigned**
Data Source
Encapsulation
Application **http**
Data **Rate**
Time Range **Last 15 minutes**
From **2015-May-18, 16:02**
To **2015-May-18, 16:17**

Application Traffic By Hosts

Show All

Row	Host	In Packets/sec	Out Packets/sec	In Bits/sec	Out Bits/sec
1	10.120.1.10	153.59	119.12	1,251,505.64	37,622.92
2	10.100.1.10	599.53	773.40	189,434.08	6,267,492.75
3	10.120.1.19	156.36	121.30	1,258,764.44	38,302.98
4	10.120.1.14	163.55	126.78	1,321,245.49	40,052.64
5	10.100.1.11	599.01	772.48	189,098.56	6,257,577.12
6	10.120.1.17	159.14	122.94	1,280,046.08	38,844.59
7	10.120.1.13	146.84	113.99	1,192,457.46	35,968.53
8	10.120.1.12	149.24	115.77	1,211,963.31	36,621.70
9	10.120.1.15	154.53	119.91	1,253,038.63	37,854.76
10	10.120.1.18	153.34	118.71	1,235,211.19	37,438.27
11	10.120.1.16	158.43	122.82	1,291,048.03	38,821.47

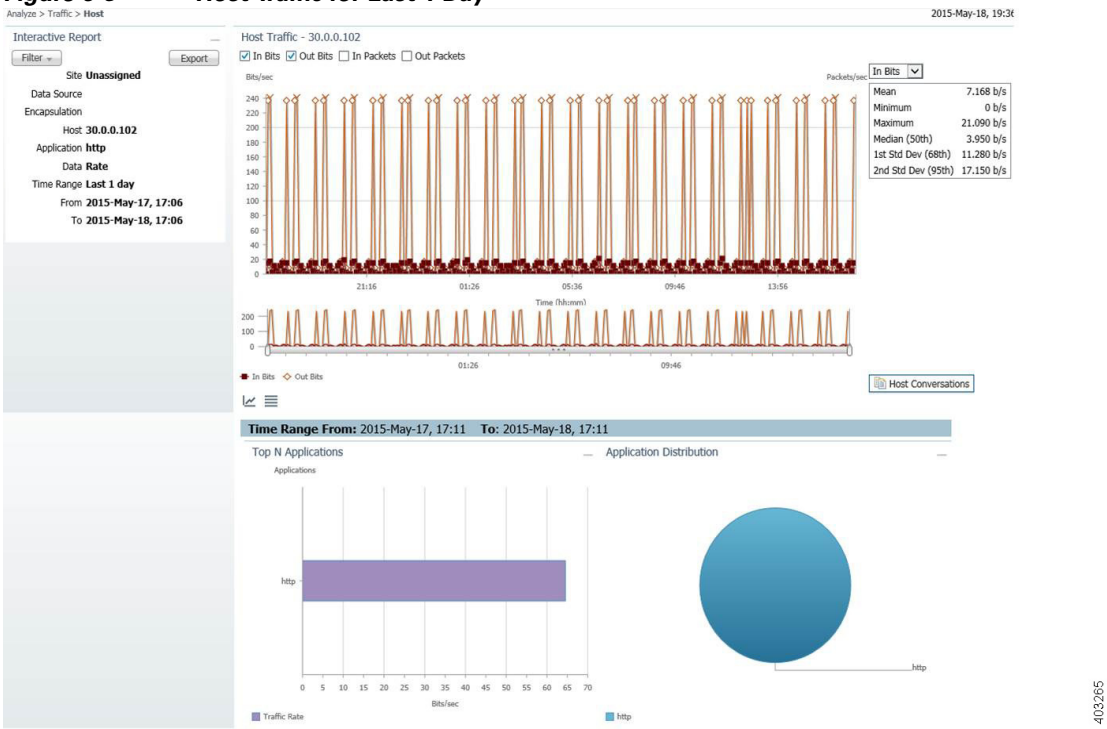
403264

Using Packet Analyzer for Historical Trends via Interactive Report

Historical trending is an important component of network performance management. While real-time analysis provides information about events, historical trending provides visibility into event sequences. Such sequences offer valuable information about various aspects of the network such as changes in network traffic behavior, anomalies and unusual activities, and network usage in peak times versus low times. It is also helpful in planning future network upgrades, application roll outs, and hardware buildouts. Here are some things to take note of regarding Packet Analyzer's historical trending capabilities:

- Use the Interactive Report > **Filter** button (located on the left side of the Packet Analyzer window) to look at short term and long term trends by changing the Time Range. The interactive reports can be exported or the filter setting saved for quick view in the future. The exported data can be sent via e-mail in CSV or PDF format.
- Figure 6-8 displays host traffic for the last day, and using the middle graph you can zoom down to the required time range to view what other application this host is using.

Figure 6-8 Host Traffic for Last 1 Day

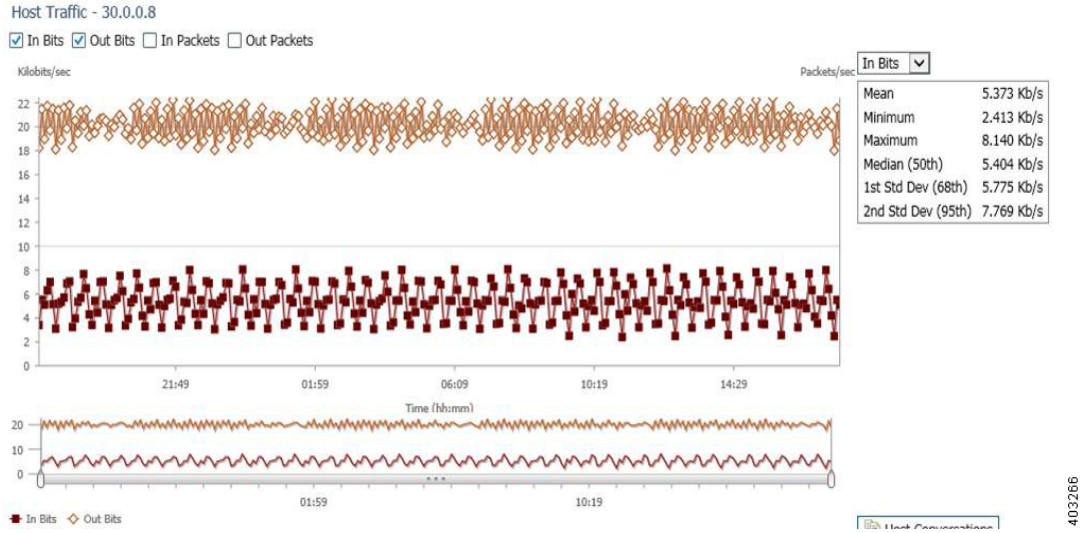


In the following deployment scenario, you will predict the capacity needed for a new branch build out due in six months by studying the usage of an existing branch office of a similar size. To deploy a Packet Analyzer located in the branch router (ISR) of the existing branch:

Step 1 Start capturing traffic rates between the branch and the data center. View the traffic for the last month from **Interactive Report > Filter > Time Range > Custom** (enter a date covering a month).

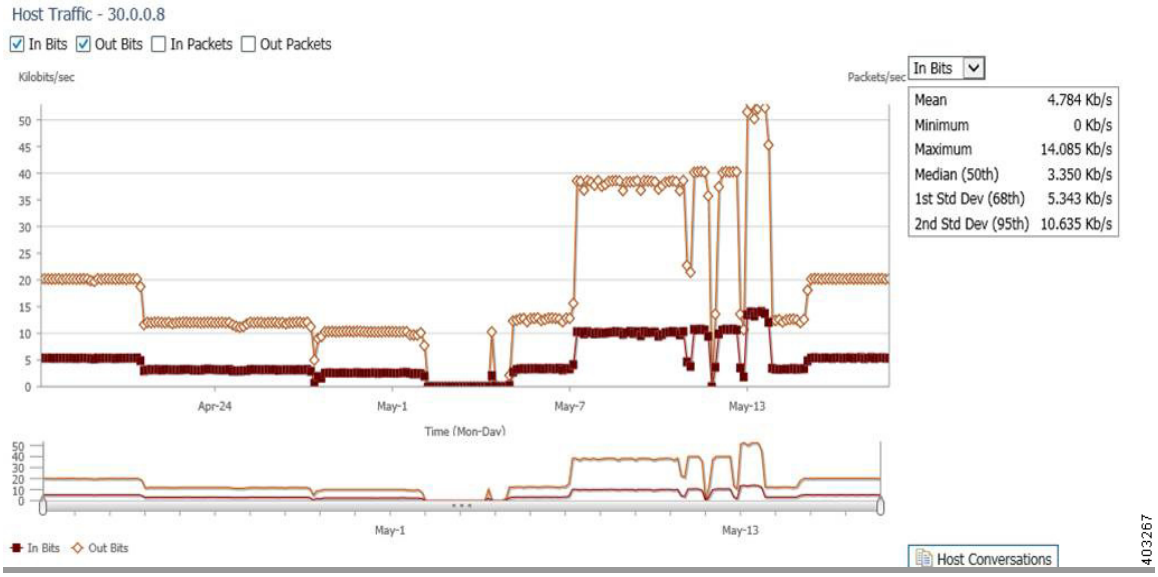
Step 2 Open a conversation report from today and find a stream that has a mildly increasing trend but is unable to confirm the rate at which it is increasing (see Figure 6-9).

Figure 6-9 A Stream with a Mildly Increasing Trend



Step 3 Change the Time Range dynamically in the Interactive Report to study the trend with a granularity of one month. You may find that the pattern does show periodic increases (see Figure 6-10). You are then able to conclude that the ISP link needed at the new site would be similar, and so a standard T1 line would be more than sufficient for the needs of the new remote office.

Figure 6-10 The Trend Shown with a Granularity of 1 Month



Studying historical trends is a valuable exercise in planning and creating baselines in a network. Monitor and trend on business critical applications and servers. These trends should provide handy information in a variety of day-to-day decisions.

Using Packet Analyzer to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications

Application Performance Response Time Analysis provides up to 45 metrics. You can configure thresholds based on many of these metrics, and receive an alert when the thresholds are passed. Thresholds should be set for critical applications or servers using Average Server Response Time, or Average Transaction Time, or Average Network Time and Average Server Network Time. These thresholds will help identify where the problem lies in the application performance, and show whether the problem is a server or network issue. Depending on the alarm, you can access the Packet Analyzer to see the applications and clients accessing the server, or to check the devices in the traffic path monitoring device and interface utilization.

See Application Response Time, page 3-21.

See Defining Thresholds, page 7-34.

Using Packet Analyzer to Evaluate Application-Level Performance Monitoring for UDP Real-Time Applications

The Packet Analyzer monitors and analyzes RTP streams and voice calls statistics by intercepting the data collected by endpoints. So, when a phone call ends, the endpoints calculate the information and send it to the Unified Communications Manager (aka the Call Manager), the Packet Analyzer collects the data (as log as it is along that path).

Packet Analyzer uses the voice call statistics from the endpoint with the RTP stream to correlate the phone number with the IP address of the endpoint. Alerts are sent based on analysis of the RTP streams for MOS, Jitter, and Packet Loss.

To use Packet Analyzer to monitor the application-level performance for UDP real-time applications:

Step 1 Set up thresholds to focus on which types of performance metrics you want to monitor at **Setup > Alarms > Thresholds**.

Step 2 View voice signaling/RTP traffic at **Analyze > Media > RTP Streams** or **Analyze > Media > Voice Call Statistics**.

See Analyzing Traffic, page 3-9, RTP Streams, page 3-33.

See Table D-31, Media Monitor Setup Window, page D-20.

Troubleshooting

Using Packet Analyzer for Problem Isolation

The alarm details (found in the Cisco Security Packet Analyzer Software under **Monitor > Overview > Alarm Summary**) provides information you can use to drill down on the threshold that was violated. You may also receive this alarm in e-mail (**Setup > Alarms > E-mail**). An example of the alarm is:

```
2013 SEPT 28 9:17:0:Application:Exceeded rising value(1000);packets;60653;Site(San Jose),
Application)
```

After receiving this alarm, you can access the Packet Analyzer GUI to view the application in your specific site to determine why there was a spike. Click on **Analyze > Traffic > Application**; in the Interactive Report window on the left, change Site to "San Jose," Application to "HTTP," and Time Range to the range when the alert was received. This will display all the hosts using this protocol. You can see the Top hosts and verify there are no unauthorized hosts accessing this application. You can also access **Analyze > Traffic > Host** to view which conversations are chatty, and therefore causing the increase traffic for this application.

If the alarm is for an Application Response Time issue, you can access **Monitor > Response Time Summary** or **Analyze > Response Time > Application** to drill down on what hosts are accessing the application. Identify the application server and view what other applications are hosted and all the clients accessing that server.

See Monitor: Using Response Time Summary, page 3-5.

See Analyze: Measuring Response Time, page 3-19.

Using Packet Analyzer for SmartGrid Visibility

The Packet Analyzer will not recognize the IEC 60870 protocol out of the box (this is one of the main protocols used by power distribution companies). You will have to add a custom protocol, because it is a specific port you will be using. When you choose **Setup > Classification > Application Configuration**, you will see all hosts using that application. It will be identified as a Telnet application.