Bandwidth Monitoring Buyer's Guide

Progress® | ipswitch®

Everyone and everything in our modern connected world uses bandwidth. The pipes are now far bigger than the old 56kbps dial-up speeds most of the world endured once upon a time, so bandwidth is usually not seen as an issue by the vast majority of network users. Well, not until there's a problem, that is.

The issue is that bandwidth is often seen as effectively 'free' by most users and yet it's not 'free' for the providers. Still, a proliferation of connected devices, apps that connect regularly for no real purpose, the Internet of Things, and the general bloat of modern software and modern business all combine to consume bandwidth almost as fast as it can be made available. Most of the time this isn't an issue, but when bandwidth suddenly becomes limited, EVERYTHING slows down. And that can cause some crucial issues. That's why it's essential that anyone responsible for any network monitors their bandwidth if they want that network to work smoothly.

This document will look at why we should be monitoring our bandwidth, what some of the advantages of monitoring are and what you should look for when choosing a tool that will monitor your bandwidth.

What is Bandwidth?

Put simply, bandwidth is a measurement of the amount of data transfer that takes place in each unit of time, i.e. 3MB/s equates to three megabytes per second. The higher the rate per second the more bandwidth you have. Note that 3MB and 3Mb are not the same things as there are 8 megabits (Mb) in a megabyte (MB).

Every device with an IP address on your network uses bandwidth. Even IoT devices using the Message Queuing Telemetry Transport (MQTT) protocol (a protocol designed to work on networks with limited bandwidth) will contribute to the overall bandwidth usage.

The most commonly used analogy used for bandwidth is based on water pressure. You have a water pipe going to your home. If you turn on the shower, the pressure is fine. But, leaving the shower running, for every additional tap you turn on in your home, the shower pressure drops, as the total water capacity available (determined by the diameter of your water pipe) is shared with multiple 'devices.'

Therefore, you must determine which devices use your bandwidth, take this information and decided on a plan of action, whether this involves assigning a max bandwidth per user, replacing hardware, cabling or leasing additional broadband connections.

Why Monitor Bandwidth?

A lot can change in a decade. In so many ways, we're living in a completely different landscape than we were just ten years ago, and workplace technology is no exception. We've moved workloads to the cloud, introduced BYOD policies, and now rely on workplace wi-fi way for all corporate provisioned devices. All of this network activity puts enormous stress on enterprise networks, and IT teams need to be able to keep track of it to keep things humming. That's where enterprise network bandwidth monitoring tools come into play.

When bandwidth suddenly becomes limited, EVERYTHING slows down.

And that can cause some crucial issues.

A high performing network is a core component of a successful IT infrastructure. To keep business processes running as smoothly as possible, network bandwidth monitoring solutions provide network administrators with the tools they need to keep track of the availability, performance and bandwidth usage of an IT network.

Monitoring bandwidth is one of the most critical aspects of network management. Without comprehensive insight into traffic type and bandwidth utilization, it is not possible to ensure proper availability of bandwidth. By monitoring bandwidth utilization, it is possible to:

- **Determine the users, applications and hosts taking up critical bandwidth**
- **Assure adequate bandwidth for business-critical applications**
- **Identify bandwidth bottlenecks such as bandwidth hogging processes unnecessarily running in peak load periods**
- **Minimize the impact of non-critical or unauthorized network traffic**
- **Assist with identifying unauthorized applications**
- **Alert potential DDoS (Distributed Denial of Service) attacks or externally initiated port-scans**

Also, remember that with viruses and malware often consume abnormal amounts of bandwidth, so monitoring bandwidth utilization can be invaluable in identifying security anomalies.

The Benefits of Network Bandwidth Monitoring

ALERTS AND QUICK RESPONSE TIMES

The value of a network monitoring solution lies in the early detection and reporting of network errors and malfunctions. With these tools, network teams no longer need to constantly manually monitor their networks as the tool will send alerts only when something needs immediate attention. Often, network administrators can be overwhelmed with alerts which can distract them from other more pressing matters. A bandwidth monitoring tool should be able to identify network dependencies to reduce redundant alerts.

With these tools, network teams no longer need to constantly manually monitor their networks as the tool will send alerts only when something needs immediate attention.

ASSIST IN NETWORK ENGINEERING

Network bandwidth monitoring can tell you a lot, and with this knowledge comes improved insight in developing and perfecting enterprise networks. By understanding the usage levels of links, network engineers can plan for extra links to avoid congestion. Network bandwidth reports help in defining the way that a network will function in the future.

IDENTIFY BANDWIDTH HOGS

The bane of every network administrator's existence; bandwidth hogs, or as I call them the 'gig pigs', gobble up bandwidth like it's their job. Using a network bandwidth monitor, administrators can identify which employees are using the most bandwidth and which applications they're using. With this information, network administrators can decide how much bandwidth each employee needs to do their job and which applications should have priority over network bandwidth.

SECURITY

What's an enterprise network without security? Despite network monitoring's reputation as an IT Swiss-Army Knife, security is one area where it's rarely used to its full potential. That's too bad because you can easily put the data and insights generated by network monitoring to good use for security purposes. Considering that 68% of all data breaches took months or longer to discover, according to Verizon's 2018 Data Breach Investigations Report (DBIR), why wouldn't you leverage a network monitoring solution to strengthen your security?

A network monitoring tool can greatly improve the security of a network and offers increased control for network teams. Network monitoring tools can tip network administrators on warning signs that may indicate a possible attack, for example, if administrators detect an unusual amount of usage on a port. Network bandwidth and traffic reports provide critical information that helps to detect traffic anomalies. Network bandwidth monitoring can quickly and seamlessly be applied to existing network security technologies such as firewalls and scanners. Some other specific applications of network monitoring to security include:

- **Discover Breaches Faster -** You can set up email notifications and alerts for changes to the configuration of network devices, and audit configuration against defined policies. You can also view and compare device configurations, and if configurations are lost, you can automate network device configuration backups.
- **Detect Cryptominers Using Your Resources -** With a modern network monitoring tool you can easily monitor for CPU spikes and set up alerts for when CPU usage exceeds 90% (or any other threshold you want) on machines that don't regularly perform CPU-intensive tasks. This is a simple way to keep track of your machines and find out if there's anything strange going on.
- **Detect DDoS Attacks and Anomylous Network Behavior -** By monitoring real-time bandwidth usage and historical bandwidth trends, network flow monitoring can proactively identify security issues like DDoS attacks, unauthorized downloading and other suspicious and potentially malicious network behavior.
- **Detect Access to the Dark Web -** You can monitor all Network Traffic Analyzer Sources and alert admins when any host exceeds a configurable number of connections to known Tor ports during a set period. This allows administrators to control access to the Dark Web by their users.

This is only the tip of the proverbial iceberg since bandwidth monitoring is the very first tool that network admins should be using to figure out what's going on in their networks. Depending upon the organization, the network architecture, the business needs, and the network traffic, there are usually a number of other advantages a savvy administrator can realize from using a bandwidth monitoring tool.

How Bandwidth Monitoring Works

How exactly do these tools monitor network bandwidth? Two main software techniques are used for collecting and monitoring network bandwidth usage data. They are:

SNMP

In this method, bandwidth monitors send SNMP queries to SNMP-enabled devices on the network. The devices then send device-centric information (stored in their Management Information Bases (MIBs)) back to the device. This information can include network bandwidth usage data. The monitoring tool can then analyze this data to monitor network bandwidth usage.

A business depends on its ability to continuously improve services to compete. Especially today, customers have an expectation of modernity and convenience that can dictate their choice of who they want to do business with. This expectation also extends how you enable your business customers to offer services to their customers, and Service Level Agreements (SLAs) often reflect this. With a capable automation tool, you can meet those SLAs and keep your customers happy.

NetFlow

NetFlow is Cisco's monitoring protocol that can collect various statistics on network bandwidth usage across devices, and hence monitor network bandwidth. NetFlow is based on "Flows," which is defined a continuous series of packets sharing common characteristics (including source/destination IP and ports, IP protocol, Ingress Interface and Type of Service values). These characteristics are defined in Cisco's NetFlow 7-ple key. NetFlow can be enabled on network device interfaces, which then monitor the "flows." A series of packets with unique values in the 7 fields constitutes a flow, and subsequent packets with identical values are added as increments to the existing flow. A difference in even one of the values is recorded as a separate flow and flows end when configurable timeouts are reached or specific flow ending packets are encountered. The flow data is then sent as UDP packets to a NetFlow collector, which then analyses the data into information for monitoring network bandwidth (including bandwidth usage, network traffic details, network trends and anomalies, bandwidth peaks and valleys, performance metrics, and so on).

How to Monitor Bandwidth Utilization

Network bandwidth is typically monitored by tools that use software technologies like SNMP, packet sniffing and flow monitoring, or through hardware probes. While SNMP, sniffing and probes can show bandwidth utilization, administrators need to have better insights into which applications, protocols, and users are consuming bandwidth. This information can be comprehensively provided by flow monitoring tools.

Administrators need to have better insights into which applications, protocols, and users are consuming bandwidth.

Monitoring tools are based on a "flow," which a series of network packets sharing common characteristics like source IP and port, destination IP and port, Type of Service, protocol etc. Cisco's NetFlow flow monitoring protocol, for instance, defines a 7-ple key, with 7 characteristics that define a flow.

Packets with identical values in all 7 fields are considered one flow, while the difference of even a single value makes up a new flow. NetFlow is enabled on an interface basis in devices. The devices collect the flow data and export it as UDP packets to an analyzer, which then analyzes and classifies data to highlight bandwidth monitoring, bandwidth usage, billing, security issues, and capacity planning.

While NetFlow is the most widely used flow monitoring protocol, Juniper's proprietary jFlow, and the multi-vendor technology sFlow are also used to monitor network bandwidth. jFlow is a technology similar to NetFlow, with just one difference. jFlow samples each ingress flow, while NetFlow samples data flow on both the ingress and egress interfaces on the device. sFlow, on the other hand, is a packet sampling technology that samples 1 in every Nth packet that passes through the interface.

This is a fairly high-level overview, but most bandwidth monitoring tools work similarly to the above. There's definitely a more detailed and technical explanation which will vary from tool to tool, but the basics aren't really going to change. Given that, the next step is to figure out what features these tools include beyond the basics.

What to Look For in Bandwidth Monitoring Software

A primary part of the system or network administrator's role is ensuring network uptime. This is achieved using available administrator tools that are designed to monitor network traffic. The tools selected will vary by organization but can include network monitoring tools, bandwidth monitoring tools, and network sniffers, all of which aid the admin in ensuring maximum available bandwidth for all users.

Such monitoring was once easier, but nowadays in addition to wired devices, there are other considerations. Wi-Fi routers are commonplace, and connected printers, tablets, laptops, and even smartphones must be monitored. Add IoT devices and sensors that use a variety of protocols, from the MQTT protocol to Bluetooth and indeed Wi-Fi and you begin to appreciate the problem.

It is generally not feasible to install monitoring software on each device thus the ideal solution will monitor the entire network at a central point, the router or main server. Some routers offer total bandwidth usage tools but lack the per device solution that is needed. Obviously, what is needed is a solution that can monitor everything, with options that allow monitoring by device, user or IP address.

A bandwidth monitor tracks bandwidth use over all areas of the network – devices, applications, servers, link connections, leased lines etc., and offers insights into network bandwidth utilization and traffics analysis. It also maps out historical trends for capacity planning and proactively identifies security issues.

Bandwidth monitoring software uses various technologies including SNMP and flow-based technologies like NetFlow, to identify, monitor, and analyze application and network traffic. Some of the key capabilities to look for in a network bandwidth monitoring tool include:

It is generally not feasible to install monitoring software on each device thus the ideal solution will monitor the entire network at a central point.

- **Real-time bandwidth monitoring, and mapping historical user trends:** Real-time monitoring allows administrators to identify interfaces/links/applications/users/protocols taking up bandwidth. For instance, the Flow Monitor can highlight bandwidth utilization over LAN, WAN links and specific devices, identifies internal and external traffic sources/destinations. It also classifies the information as Top speakers, Top Protocols, Top Applications that use up bandwidth.

- **Protocol Support:** Bandwidth usage and bandwidth availability monitoring are essential features for a network monitoring solution. That being said, it's critical for IT teams to keep an eye out for solutions that support the most common protocols such as SNMP, jFlow, and NetFlow as well as helping organizations meet governmental and industry regulations.

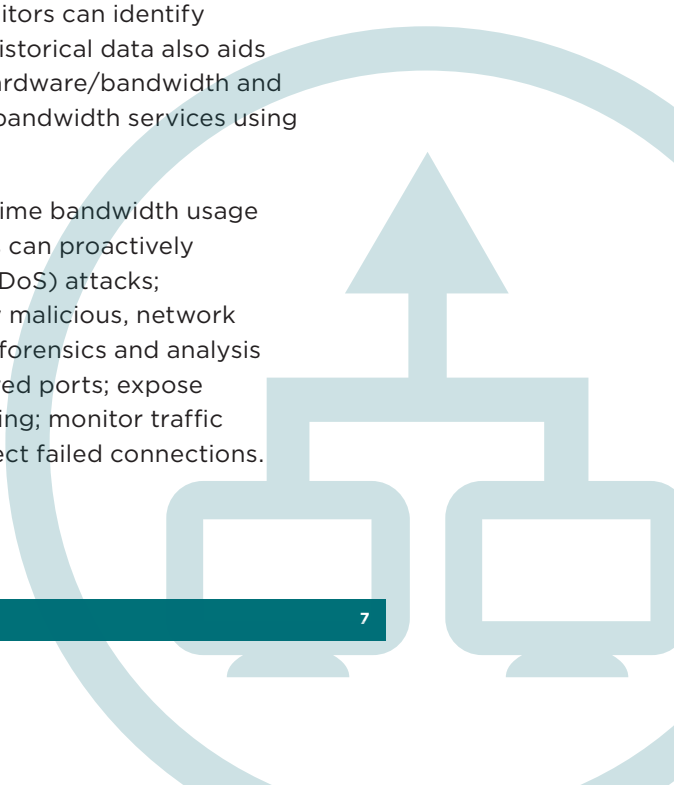
- **Alerts:** Additionally, the importance of timely and relevant alerts cannot be stressed enough. A solid network bandwidth monitoring tool allows admins with the ability to customize and craft alerts that meet the organization's unique needs. Alerts can be sent to admins through email, text message, and whole list of list of additional methods. When looking for a powerful network monitoring tool, alerts and alarms should allow administrators to define dependent actions to avoid multiple alerts for a single server crash.

- **Apply QoS policies:** By default, each network channel operates on a best-effort basis – every application gets equal priority, be it a business critical VoIP service, or a user streaming video content. QoS policies are essential to ensure business-critical applications get sufficient bandwidth. WhatsUp Gold, for example, verifies Quality of Service over through Type of Service (QoS over ToS); DSCP for LAN/WAN, CBQoS policies and Cisco NBAR classification mechanisms.

- **Archives:** A full-bodied networking monitoring solution offers network administrators insights and information related to the performance of bandwidth in easy to digest and analyze dashboards and lists. All network related data should be archived so that network teams can look back to see how bandwidth usage and network performance changes over time.

- **Historical trends identification:** By studying traffic patterns and usage over a period of time, and by analyzing the data, bandwidth monitors can identify trends in bandwidth usage and potential bottlenecks. The historical data also aids administrators in capacity planning; efficient purchase of hardware/bandwidth and also verifies bandwidth-based billing including "burstable" bandwidth services using 95th percentile reports.

- **Identify abnormal bandwidth usage:** By monitoring real-time bandwidth usage along with historical bandwidth trends, bandwidth monitors can proactively identify security issues like Distributed Denial-of-Service (DDoS) attacks; unauthorized downloading and other suspicious, potentially malicious, network behavior. For instance, the Flow Monitor can aid in security forensics and analysis by automatically identifying high traffic flows to un-monitored ports; expose unauthorized applications like file sharing and video streaming; monitor traffic volumes between pairs of source and destinations; and detect failed connections.



- **Virtual Network Monitoring:** The modern enterprise is much more reliant on cloud technology and virtualized network to keep businesses processes running. In today's cloud heavy environment, a good network monitoring system should offer methods for keeping tabs on systems such as VMWare, Microsoft Hyper-V, Parallels Virtuozzo Container or Amazon Elastic Compute Cloud.
- **Integrated Clusters:** Integrated Clusters improve network security in terms of downtimes of the monitoring tool. With this feature, administrators are equipped with parallel network monitoring by using a variety of instances from the monitoring tool. To illustrate how this may come in handy, imagine that one of these instances fail, the other instances will step up and take over their tasks without any interruption. This, in turn, keeps network users from possible software failure.

There are, of course, additional capabilities that your organization may require or that would be useful depending upon your network and the type of traffic running across it. That said, the above points are a good place to start and can be used as a checklist when assessing and comparing network bandwidth monitoring tools.

Choosing a Network Bandwidth Monitoring Tool

As mentioned previously, your selection of bandwidth monitoring software and related add-ons will depend on your network infrastructure and the devices connected to it. There is no single best bandwidth monitoring software, in the same way, there is no best screwdriver for disassembling a laptop. Your aim is to optimize network traffic by using the correct combination of network monitoring tools to reach your goal. The reduction of unnecessary bandwidth consumption is an additional goal. Your network administrator will also use performance monitoring tools to achieve maximum network performance, identifying problem areas as they arise.

Your chosen solution should have the ability to monitor the bandwidth of all the devices connecting to your network, regardless of type, platform or connection protocol used. It should verify that your total available bandwidth coincides with the speed agreed with your provider. It should also be able to check off most (if not all) of the key capabilities listed in the previous section. The next step is to take a look at the many solutions on the market (we obviously have our favorite choice). Unless, of course, you think it's a good idea to try building your own.

DIY vs. Commercial Solutions

It can be tempting to build your own DIY network bandwidth monitoring solution, but what's the real cost of building and maintaining such a tool at scale?

For many start-up IT services organizations, Managed Services Providers (MSPs), and even in-house IT departments, it can be very tempting to build your own monitoring solution. This can be for a variety of reasons of course: there could be no budget available to procure a Commercial-Off-The-Shelf (COTS) solution, or maybe there's an organizational belief that the team has the skills to build exactly what your organization needs to serve your internal and/or external customers.

A DIY build of a monitoring tool is usually not formally planned—it just starts and evolves as your customer's requirements dictate. Over time, it usually becomes the responsibility of a very small number of people, or even a sole individual, within the organization who becomes the owner for the homegrown tool. Having met with many different organizations, ranging from large System Integrator organizations to mid-sized boutique IT services organizations, small MSP companies, and in-house IT organizations, one thing they all agreed is

that ongoing maintenance of such tools can consume a considerable amount of at least one, but usually a few people's time. We cannot ignore the old adage that time equals money. What initially started as a good initiative—build a tool to automate and manage repetitive bandwidth monitoring tasks—can quickly turn into a constraint on your organization. Smaller organizations have reported that, on average, one of their skilled IT operations personnel needs to spend up to 40% of their time maintaining their homegrown tool.

So let's think about the "whole-of-life" costs of building an in-house tool. There are at least 3 cost elements that need to be factored in: build cost, maintenance cost, and opportunity cost. There's also a transition cost—more on that later.

CALCULATING BUILD COST FOR DIY NETWORK MONITORING

The cost of building the initial version of the tool is often not pre-calculated, but let's assume for a small IT services organization they allocate one experienced IT operations engineer for 50% of his or her time to develop a tool over a period of 6 months. If that engineer has a $50k salary/benefits cost. The initial Build Cost is therefore $12,500 ($50,000 x 0.5 x 0.5).

...THE COST OF MAINTENANCE

Given the constant rate of change in the technology sector, it's reasonable to assume that up to 30% of an engineer's time will be needed to maintain and update the in-house monitoring tool—which would include adding new functionality to meet ongoing customer needs. The annual maintenance cost would therefore conservatively be $15,000 ($50,000 x 0.3).

AND THE OPPORTUNITY COST

This is usually a "hidden" cost that many organizations fail to factor in at all. IT services organizations and many in-house IT departments charge their customers a fixed hourly or daily rate for their qualified engineers. So again, let's assume that one of the IT engineers is spending 30% of their time annually maintaining the in-house tool. We can make the following additional assumptions based on what would be typical industry norms:

The engineer's Daily Charge Out Rate is **$400/day**

The number of billable days per annum per engineer is **220**

The opportunity cost, or "lost revenue" that your business has missed out on because of your engineer maintaining your in-house tool is therefore **$400 x 220 x 0.3 = $26,400**

So let's stop here and reflect for a moment on the actual costs so far.

Initial tool build cost	**$12,500**
Annualized ongoing cost for the tool (Maintenance cost + Opportunity cost)	**$41,400**

Many organizations fail to factor in the true cost to their business of maintaining a home-grown tool. Enlightened organizations, when they realize this, usually make a decision to procure a COTS solution. But this again introduces yet another cost – what we have referred to as a TRANSITION cost. This needs to consider items such as:

- **Vendor evaluation and section process (which could include an RFP phase) for a new COTS solution**
- **Installation and configuration of the chosen COTS solution and user training**
- **Migration / transition of customers from the in-house tool to the COTS solution**
- **Ongoing administration of the COTS solution**

There will always be a healthy debate about whether to build or buy a tool. However, it is important to bear in mind that while it might appear cheaper to build your own homegrown network bandwidth monitoring tool, the true cost can be much higher than you expected.

Conclusion and Next Steps

We've outlined what you should be doing and why, but the final step is likely the most time-consuming: choosing a bandwidth monitoring tool for your entire networking environment. Of course, we have our own opinion on the most effective tool out there, but it's important to review the options available. Use the above key features as a checklist to determine if the solution you're considering is going to do what you need it to.

The next step is to leverage those capabilities to improve your network and the experience of your end users. Remember that network bandwidth monitoring will help you ensure application performance, oversee network traffic prioritization policies, and save money by eliminating costly bandwidth utilization issues. Your network bandwidth monitoring tool should also allow you to:

- **Configure flow enabled devices automatically**
- **Determine exactly which users, applications or hosts are consuming network bandwidth**
- **Track and resolve network traffic or congestion problems**
- **Ensure critical business applications get the bandwidth they need**
- **Measure bandwidth usage**
- **Verify ISP providers billing**
- **Plan for spikes in usage to avoid dropped packages or delays**
- **Receive real-time alerts on bandwidth usage violations**
- **Secure your network**
- **Identify the introduction of viruses and worms**
- **Detect DOS attacks and other rogue activity directed at your network**
- **Monitor the network for unauthorized application usage; easily detect streaming audio, video, or file sharing applications**

In addition to taking full advantage of your network bandwidth monitoring solution, there are a few other next steps that go beyond software implementation that you should consider. All of these can help you control your bandwidth consumption:

Educate the Most Wasteful

Not only must you deal with an expanding userbase; you also have to field new applications and services your organization needs. This wouldn't be so bad if these apps and services didn't require their own share of bandwidth in order to function, or if file sizes stayed the same across each machine using them. You can't expect users to always know how to minimize content size before sending it, or when not to use the heaviest programs. You need to include information about the consumption of bandwidth when users receive new hardware or software.

You can't expect users to always know how to minimize content size before sending it, or when not to use the heaviest programs.

For example, one employee has to send a large volume of high-res images. Do they know how to modify those images so that they consume less bandwidth? What's even worse is when your users decide to send these large files via email. You know email attachments are sent using MIME (Multipurpose Internet Mail Extensions), but the rest of your office may not. Because MIME uses as much bandwidth as it sees available, getting your users to use managed FTP instead would be beneficial for all involved.

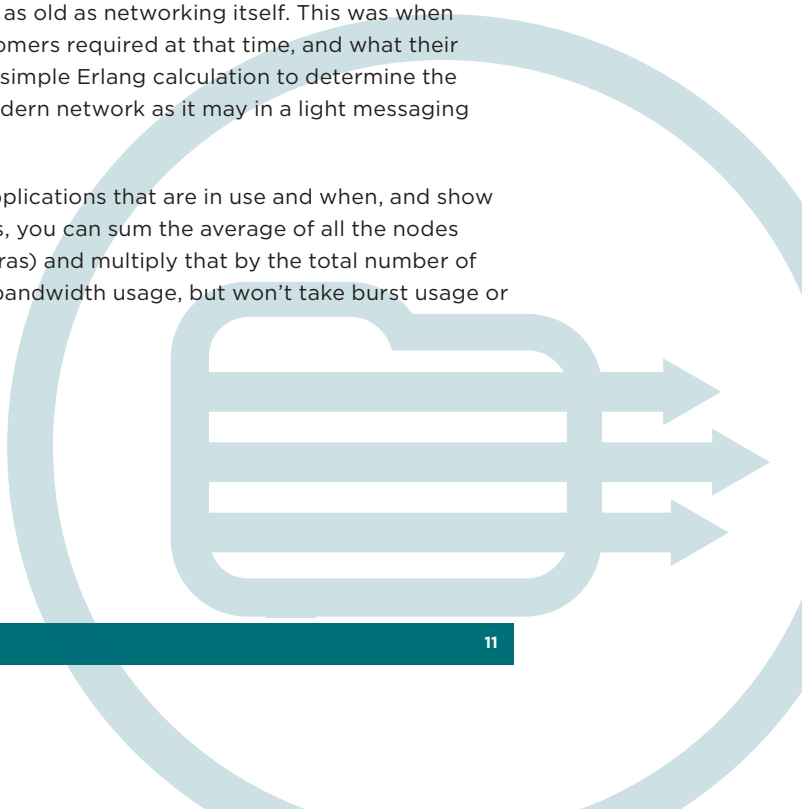
When Implementing VoIP, Tread Lightly

Your phone system is also likely eating up a lot of available bandwidth. This places an even larger load on your network than oversized attachments. There are a number of reasons for this. The main cause is in IP telephony, which requires packets to transfer in a more dedicated fashion than pure data. If you're getting ready to perform a bandwidth usage calculation and your company wants in on VoIP, you need to know what codec the system uses so you can gauge how much bandwidth is on the bubble. You might also want to assess and monitor network performance levels including call quality including jitter, latency, and packets. Yet VoIP is just one of the network bandwidth usage hogs you've got to put up within your network. Chances are you've also considered video conferencing apps, such as GoToMeeting and WebEx. You may have also decide to add building security functions like surveillance cameras connected to the network. All of these are drains on your available bandwidth. We need not even mention the pressure mobile places on your network as your organization rolls out a BYOD policy — but there it is.

Calculate Bandwidth

Calculating the bandwidth your network needs is a challenge as old as networking itself. This was when engineers needed to know what sort of bandwidth their customers required at that time, and what their needs might be in the future. They used to be able to make a simple Erlang calculation to determine the network architecture necessary. This won't do as well in a modern network as it may in a light messaging app, though, according to Fast Company.

Instead, make sure the monitoring tool you use can list the applications that are in use and when, and show their network usage over time. Once you've got these metrics, you can sum the average of all the nodes on your network (don't forget to include devices like IP cameras) and multiply that by the total number of nodes on-site. This will give you a decent estimation of your bandwidth usage, but won't take burst usage or excessive MIME attachments into consideration.



Segment Your Network (Properly)

Even in a midsized organization, chances are you're already segmenting your network. This decreases the traffic across the whole network by dividing it logically — by department, for example. You can do this either physically using intelligent switches or by using sub-nets. If you're on a tight budget, sub-netting is your best bet because it only requires a computer configuration change instead of new hardware.

Finally, if you aren't certain about any of the above or still aren't sure exactly what you should be using to monitor your bandwidth, ask. There are millions of other admins in the same situation you are and they're usually happy to share their experiences. Check out the customer forums for the vendors on your short list to see what the owners of those solutions like, don't like and how they're using them. If nothing else, go ahead and call up the vendors themselves and ask them how they'll meet your requirements. You'll be surprised at how often your biggest problem has already been solved by someone else that's happy to share their knowledge.

About Progress

Progress (NASDAQ: PRGS) offers the leading platform for developing and deploying strategic business applications. We enable customers and partners to deliver modern, high-impact digital experiences with a fraction of the effort, time and cost. Progress offers powerful tools for easily building adaptive user experiences across any type of device or touchpoint, the flexibility of a cloud-native app dev platform to deliver modern apps, leading data connectivity technology, web content management, business rules, secure file transfer, network monitoring, plus award-winning machine learning that enables cognitive capabilities to be a part of any application. Over 1,700 independent software vendors, 100,000 enterprise customers, and two million developers rely on Progress to power their applications.

Learn about Progress at www.progress.com or +1-800-477-6473.