

Performance

My network is slow, what do I do?

The key to resolving this is knowing what not to include. For instance, if the slowness occurs for local servers and Internet traffic then the Internet and WAN issues can be eliminated. Assuming this is a matter of local network only, rule out items one at a time from the source of the packet (e.g desktop) to the destination (server). For instance:

1) Local desktop or laptop

- Make sure performance isn't hampered by virus or malware
- Make sure the network interface card isn't generating errors
- Check for bad Ethernet cable
- Check speed/duplex settings

2) Local switch

- Check speed/duplex settings
- Check port statistics for errors
- Check local patch cable
- If multiples switches or stackable switches, make sure there are no loops
- Make sure there are no broadcast problems (all ports blink at same time very frequently)
- Is there multicast video on the network

3) Local server

- Check speed/duplex
- Recheck cable
- Check network interface card
- Check server load

In numerous cases, poor local network performance is due to speed and duplex settings. Both ends should be set to auto or both ends should be hard set to same settings (e.g. Gigabit, full-duplex). MANY problems with local networks are due to speed/duplex on the endpoints or between switches.

Many network problems can be resolved by getting rid of old stacked or interconnected switches with oversubscribed uplink ports and replacing them with high-performance chassis based switches.

Read our [article](#) for more information.

Please [contact us](#).

My Internet is slow what do I do?

Many things can affect this, while WAN speeds tend to be orders of magnitude slower than LAN speeds, the first thing to do is make sure there isn't a local LAN problem such as speed/duplex mismatch. Many people and ISPs incorrectly keep adding bandwidth with mixed results without first determining how the bandwidth they do have is being used. You first need to determine actual use, don't be fooled by ISPs (especially local cable companies) and their reports of temporary "spiked" usage. By their very nature a WAN should spike at times at 100%, the issue is how often and for how long. We've seen some problems with certain cable technologies creating very poor WAN performance under load leading to very long latency.

You first have to determine:

Problem Solver

- How much bandwidth you purchased? (e.g. a T1 circuit is 1.544 Mbps)
- How much bandwidth is your WAN delivering?
- How much bandwidth are you consuming on a daily and hourly basis?

If the bandwidth is being very underutilized, then make sure it isn't a local problem or one with the server or service you're using. Use www.speedtest.net to determine what your circuit can do at various times during the day, be aware that there is almost always some kind of traffic running on your circuit that will affect the statistics. Realize that there are symmetric and asymmetric (different upload/download) solutions out there.

Assuming then that the bandwidth is being consumed, the next question is to determine how it is being used and by whom. There are many ways to tackle this including URL filtering, proxies, UTM firewalls, application aware firewalls, QoS solutions, or even an assessment by us. Perhaps the simplest is one we offer that runs on a PC with a sniffer port and gives visibility into the amount of bandwidth being used hourly, types of traffic by port/service, who is using the traffic along with policy and appropriate use considerations. For a free trial of the software, [contact us](#). This is far easier to use than a Wireshark with too much detailed packet information or a URL filtering tool that doesn't show all traffic.

Please [contact us](#).

My videoconferencing and IP telephony is unreliable, garbled and unpredictable, what do I do?

Assuming it's not issues with local LAN and WAN issues of earlier questions. This is either a problem with competing traffic needs or jitter, two things dramatically affect video and audio quality. Bandwidth is required so that there is adequate throughput to handle the audio/video needs along with any competing traffic. Latency is rarely looked at and affects delays due to speed of light and network equipment. When it comes to audio/video, latency is a killer. Human hearing is very sensitive to making sure packets arrive quickly and in the same order. We've all been on cell phones and other systems where it seems like both parties are talking over each other because there is a gap that's too long. Jitter is the variation of latency. Latency in of itself is a problem, when it varies tremendously on a call, it's extremely detrimental as are lost packets. Audio uses UDP, so packets are not retransmitted, dropped packets are just lost and hence voice will often sound garbled as chunks are lost.

When doing audio/video, circuit quality and consistency are key. That's why we offer a solution for making sure on critical circuits that packets always arrive in original sequence and jitter is minimized.

Please [contact us](#).

My remote offices complain about slow corporate resources, what can I do?

We're going to start with assuming it's not a general LAN or WAN issue previously addressed. WAN circuits are far slower than LAN circuits by large orders of magnitude, 100:1 is neither unheard of nor the extreme. This creates challenges when corporate networks between offices are extended across WAN circuits. It's not just bandwidth. It's about maximizing and prioritizing the bandwidth that is available and tackling the problematic latency issues. Buying excess bandwidth is not only costly, it probably won't tackle the problem and at best temporarily mask the problem underneath. Many home VoIP users have experienced poor call quality during a sudden burst of Internet use, this is a prioritization problem that needs to be addressed with QoS (Quality of Service). Large file transfers and/or backups can experience tremendous savings with WAN acceleration solutions that

Problem Solver

compress traffic. Chatty and problematic protocols like file serving and Microsoft Exchange (MAPI) behave very poorly when latency is a factor due to geographic separation and speed of light impact on latency. Poor quality circuits for satellite circuits to third world countries with poor circuit service are subject to problems due to retransmissions.

All of those problems are fairly easy to solve with WAN acceleration solutions and easy to determine the savings that might occur by actually deploying an evaluation. Find out more about our [WAN acceleration](#) solutions.

Please [contact us](#).

I need a backup to my private MPLS circuits, what are my options?

We highly recommend link balancers. Depending upon if you are using all private circuits for primary/backup, just VPN or a hybrid mix, the solution will vary.

I need to add PoE (Power over Ethernet) or change out my switches, where do I begin?

PoE is a common solution these days especially when dealing with video wireless networking. Most switches now offer PoE on all or some ports. If you have older infrastructure without PoE, line injectors can be used to inject PoE into cables on ports that don't have PoE. We also have a variety of very high-performance switches that can virtually stack or use chassis based solutions for substantially better performance than has been previously available. This includes 10 Gigabit (10 GbE) solutions. Our higher end solutions offer full line rate nonblocking solutions for the absolute best high-performance solutions for demanding environments.

Keep in mind there are several classes of PoE that deal with different wattage needs. Some lessor switches also have power management concerns that affect just how much the aggregate needs are of all the PoE ports.

Please [contact us](#).

Management

I can't tell what is up or down in my network, what can I do?

We use a variety of solutions to help automate the monitoring of systems, network infrastructure and key services and applications running on those servers. Notification includes alerting and escalation. Historical records of kept of uptime to help with management reporting. Information includes performance monitoring and resource utilization as well.

Please [contact us](#).

Is there a better way to manage TCP/IP addresses than a Microsoft Excel (or similar) spreadsheet?

You bet, this is the field of IPAM (IP Address Management). You're not alone, over 90% of the prospects we talk to still use spreadsheets to manage their addresses, that's unfortunate. Our solution based upon [Infoblox](#) allows for additional fields such as asset tags, department names, location, lease expiration, whatever you can imagine. This can also include an automated discovery that detects unauthorized changes.

Please [contact us](#).

I need to log things happening on my network, where do I begin?

The first question is to understand why the logging is needed. If this is for compliance or legal concerns, requirements will be different. We always encourage customers to crawl before they walk and before they run. Start initially with syslog solutions (we sell solutions for small, medium and large enterprises) and then branch off into more elaborate solutions for tracking database use, file server use, IM (Instant Messaging), Email and other applications.

Please [contact us](#).

How can I tell what my network is doing?

This is actually a complex question. Lets start with some basic concepts and go from there. At a detail level, Wireshark can be used on any given port or VLAN depending on what kind of port mirroring switches in place can do we also have other inspection, but it comes down to visibility and management at a higher level. In order to do that, logging should be in place to centralize all alerting from networks and servers using syslog and similar tools. This then gives visibility to alerts, alarms, notifications and such via events, that's fine for some kind of problems, but doesn't give a feel for what traffic is going where. Next is flow based data to get visibility into who is talking with whom, basically a top talkers like kind of view based upon sources, destinations and services (ports). The right kind of routers and high-end switches can provide this visibility. Switch port statistics can be retrieved via SNMP. All this data can be viewed in a network management station such as Juniper [STRM](#) including network behavior analysis based upon anomaly detections from known baselines.

Please [contact us](#).

How can I tell who is using my network?

Who is actually a different question than what. Who is based more upon network browsing characteristics and tied to desktops and laptops versus servers and other devices. Using URL filtering with user authenticated tracking helps for Internet based data and then using a tools with user awareness can help as well.

Please [contact us](#).

What is my switch port utilization?

It depends on how many ports and switches you have and the manufacturer of the switches and their capabilities. If the goal is to determine asset utilization when dealing with thousands of ports, we have solutions that can assist with this.

Please [contact us](#).

Compliance

I need to archive Email or make eDiscovery less painful, what are my choices?

Great, we offer both hosted (cloud computing based) and on-site appliances.

Please [contact us](#).

I am concerned about compliance (HIPAA, PCI, SOX, GLBA, etc.), how can you help?

Please get in [contact](#) with us so we can determine your exact requirements and realistic budgetary realities.

General and Other

I've been asked to investigate hosted or cloud computing for Microsoft Exchange, SharePoint and other applications, what can I do?

Call us, we offer managed cloud computing based solutions for Microsoft Exchange, SharePoint and other applications.

Please [contact us](#).

I was told the network was slow last night, how can I figure out why?

It all comes down to network visibility and management. First determine if the majority of problems are with LAN or WAN access. Several solutions are available, these vary from counter based for a selected time period to show what was occurring within your network to full packet capture to replay selected sessions. Prices vary immensely, so it's important to understand the need and budgetary constraints.

Please [contact us](#).

I need to look into DR (Disaster Recovery) or BC (Business Continuance), what should I do?

We use a variety of solutions to replicate existing services and data that may include various forms of automation.

Please [contact us](#).

I need to implement virtualization, what should I do?

Please [contact us](#).

How can I make sure my desktops are kept current, especially for remote and traveling users?

There are many approaches to this, these include:

- Using agents on desktops controlled with GPOs
- If you're looking at NAC, using automated methods to assess the endpoints
- If you're looking into remote access via solutions embracing [SSL VPN](#), this is also an easy and viable option.
- Lastly use vulnerability scanning solutions to validate patch levels.

Please [contact us](#).

I need to add wireless, what should I be concerned about or do?

Wireless is easy to setup and deploy, but harder to manage and secure unless it's done correctly and using the best technology. Interference is a real concern and managing the RF spectrum is a

dynamic process.

Please [contact us](#).

I have branch offices (retail, banking, commercial, etc.) and want wireless to be seamless between locations, how can I do this?

Please [contact us](#).

How can I access my corporate network remotely?

It comes down to understanding if the remote users are in offices (branches, etc.) or roaming managed or unmanaged laptops. We're big fans of [SSL VPN](#) and you can tell by our customer [raves](#), they love our solutions and talent. We encourage an evaluation process if you need the support of your management.

Please [contact us](#).

What is UTM and will it meet my needs?

UTM - Unified Threat Management, unfortunately an overused term. This tends to embrace adding additional features on firewalls such as: IDS/IDP, web filtering, application control, QoS features, SPAM control, AV (Anti-Virus), content filtering, etc.

Will it meet your needs, yes, no, maybe. Basically it depends. We always equate this to a fax/printer/scanner/copier, it does many things marginally and none all that well. If you're a small environment or have basic needs, UTM may work for you.

However, if you're a larger environment or have demanding or compliance based requirements, UTM might not meet all your needs. We do sell very high-end application aware firewalls and other solutions to address all these needs.

Please [contact us](#).

Security

How can I stop guests from plugging into my network?

Kick them out, I'd like to sometimes at least. There are a variety of methods all circling around using a wireless just for guest access or using a type of NAC solution for wired ports. We highly encourage NAC at this time. Please read our [article on NAC](#).

Please [contact us](#).

My internal or Internet facing web servers and other systems complain about security certificate errors, what can I do?

Install a certificate. We sell very affordable certificates from long-time trusted CAs. These can be purchased in one year, two year or even five year increments.

Please [contact us](#).

How can I tell if I'm secure?

Problem Solver

Long answer, but it starts with assessing your environment. There are several factors including wired, wireless, physical security and social engineering. From the wired and wireless perspective, it starts with assessing the environment by doing:

- Vulnerability scans
- Analysis of topology and firewall policies
- Doing risk mapping

We're not fans of starting with penetration testing, read our [article](#) to find out why.

Please [contact us](#).

How can I stop or get rid of SPAM?

Relatively simple these days and several choices including cloud based and on-site appliances.

Please [contact us](#).

How can I block viruses, spyware and malware?

First by understanding your environment. There are reasons to deploy endpoint, gateway and remote solutions including multiple layers. When it comes to threats, we believe in in-depth security.

Please [contact us](#).

How can I tell what people are accessing within our corporate network?

We'd suggest either looking at counter and flow based solutions using network switches and routers or using tools that enable user based tracking.

Please [contact us](#).

How can I tell what people are accessing across the Internet?

Use URL filtering solutions. We offer various solutions based upon your needs and budget.

Please [contact us](#).

I need something better and stronger than passwords, what can I do?

Look into strong authentication solutions that include two factor. Factors can be based upon:

- Something you know (e.g. password)
- Something you have (certificate on a device or something you carry like a token or proximity card)
- Something you are (biometrics like fingerprints, retina scan, etc.)

Two factor literally means two factors from above, such as something you know (password) and something you have (token).

Additionally we offer some newer solutions:

- Picture based recognition using a grid of faces
- Keyboard pattern recognition that addresses two factor compliance without tokens

Please [contact us](#).

How can I secure against Web 2.0 and social networks?

If you asked the question, that's a great start, you understand the problem. Simple URL filtering is not enough. We offer excellent solutions that are very application aware.

Please [contact us](#).

How can I prevent key information from leaving our network?

This involves using DLP (Data Leak/Loss Prevention) solutions. It depends upon how many paths we need to monitor such as:

- Email
- FTP
- IM (Instant Messaging)
- P2P (Peer to Peer)
- Web mail
- Twitter
- Web file sharing
- Etc.

It also depends where the data originates, such as file servers.

Please [contact us](#).

I've been told we have to add an application firewall, what is it and how do I do it?

Normal firewalls only inspect the ports, they do minimal inspection of the actual traffic contents (payload).

Application firewalls, especially for compliance (PCI, HIPAA, etc.), are specialized solutions that look further into various forms of attacks typically tailored for web hosted applications including databases. These attacks and security needs might include:

- SQL injection
- URL rewriting and obfuscation
- Cookie signing
- Cookie encryption
- DoS (Denial of Service) protection
- Data Loss Prevention including credit card numbers, SSNs, PII (Personally Identifiable Information) and pattern matching.

Application firewalls vary in price and capability.

Please [contact us](#).

I'd like to make sure people are allowed, but challenged, before they go to certain sites, how can I do this?

This is referred to as coaching, we offer solutions that can enable this.

Please [contact us](#).

I'd like to limit, not entirely block Internet usage during certain hours or for certain users,

how can I do this?

Absolutely, we offer solutions that can account for time of time and types of users.

Please [contact us](#).

How can I tell who has read or deleted files from my file server?

By using solutions that track file server usage for what is commonly referred to as unstructured data (not in a database).

Please [contact us](#).

How can I better manage Microsoft folder and user security?

Please [contact us](#).

I'm concerned about who is accessing our databases, what can I do?

We offer solutions that enable database logging and without installing software on the database servers.

Please [contact us](#).

I've been told we have to add an IDP, how do I do this?

Please [contact us](#).

I need to protect against a DoS (Denial of Service) attack, what do I do?

Please [contact us](#).

I need to add a DMZ, how do I do this and what is a DMZ?

We strongly encourage this, in fact we encourage multiple DMZ zones.

A DMZ stands literally for Demilitarized Zone. It's a no man's land, not part of the trusted computers and not in the Internet, it's a land between the two. A DMZ should be used to place public facing servers (e.g. web server). The understanding is that these servers could be breached at some point and should not be within the trusted portion of the network.

We encourage multiple types of DMZs for further containment of threats. A single breach in a DMZ can lead to all servers in a DMZ being breached.

We strongly discourage the use of NAT (one on one) or virtual port mapping to servers within a trusted LAN. For instance if you have a simple firewall setup with two interfaces, one to the Internet and one to the corporate LAN and public servers are within the same corporate LAN (using NAT or virtual port capability), this leads to a leapfrogging threat. Any single public server that is breached can be used as a beachhead to leapfrog attack into all other internal servers.

Firewalls are very affordable and DMZs are easy to setup.

Please [contact us](#).

Problem Solver

What is 802.1x and what does it mean to me?

802.1x is a standard that switches can use for NAC (Network Admission Control). Please read our [article](#).

Please [contact us](#).

[Contact us](#) for more information or assistance.