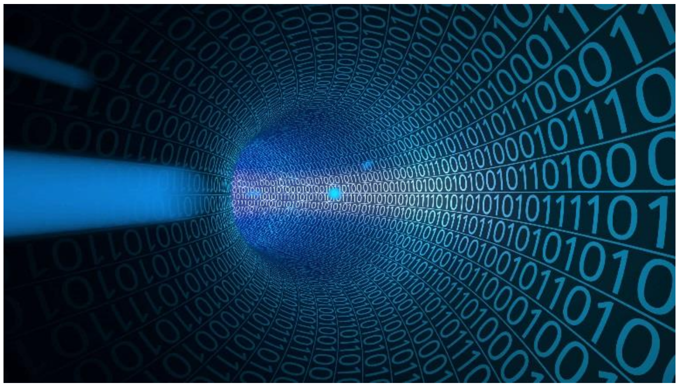
VoIP and the Customer Premises:

Solutions for VoIP Firewall Traversal, QoS, Security, and Monitoring

Peter Sandstrom, Chief Executive Officer, Cyclix Networks

Rev—181017



VoIP telephony products are now common place, with hosted VoIP products making up the majority of business telephone offerings today.

One of the main reasons for hosted VoIP's popularity is that it eliminates the need for the business to purchase a Private Branch Exchange (PBX).

With hosted VoIP the business utilizes a cloud-based phone system provided by the hosted VoIP carrier. The client is then responsible for acquiring phones, placing them onto the enterprise LAN, and provisioning them to work with the remote (hosted) phone system.

So, all one needs to do is buy a phone, plug it in and go. That's the idea anyway. The reality for most cases is a bit different.

All hosted VoIP products suffer from three core problems. They are …

Quality of Service

In the vast majority of cases VoIP shares the same broadband Internet circuit with all other bulk data services within an enterprise. However, nowhere is this voice application data stream prioritized over other data. This leaves voice competing with video, livestreaming and file data on a bandwidth-constrained IP circuit.

The end result is that oftentimes the voice quality suffers on calls made over this sort of setup. Calls become degraded and corrupted due to delayed or dropped packets, frequently to the point of having the call drop connection.

Firewall traversal

A second major issue is to how to get the VoIP service, hosted or otherwise, working through the corporate firewall. The vast majority of firewalls make no design provisions for VoIP, so it becomes an engineering task for the customer to figure out how to make it all work.

Some clients can figure it out, but most cannot. It’s not a trivial configuration exercise, and hosted VoIP carriers generally offer little or no assistance, as every customer’s internet firewall is different.

Security

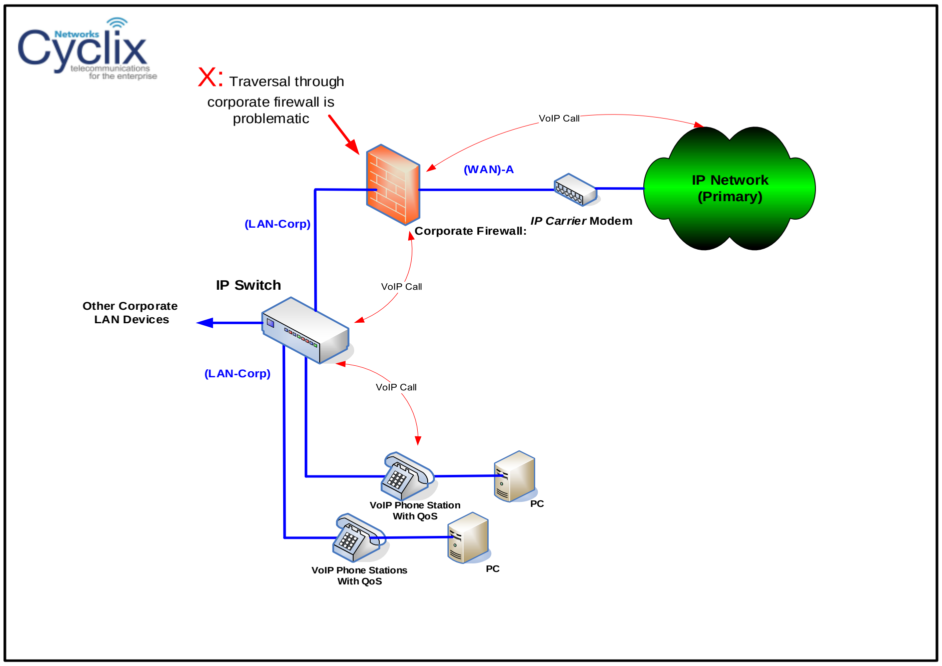
VoIP is a high-value service, and so one that is very attractive to hackers and thieves as there’s huge money to be made if one can hijack a client’s VoIP infrastructure to launch fraudulent calls from that client’s equipment.

Fortunately, there are solutions for all three of these issues if some engineering and design is placed at the customer premises. Cyclix Networks has engineered a solution that sits at the customer premises to resolve these critical issues.

The Firewall Problem

Let's explore all of these issues by starting with the firewall traversal problem. Below is a diagram showing how one would hook up a hosted VoIP phone to one's internal corporate IP network.

Following the call path for an outgoing call in this setup…


Networks Cyclix telecommunications for the enterprise
X: Traversal through corporate firewall is problematic
VoIP Call
(WAN)-A
IP Network (Primary)
(LAN-Corp)
Corporate Firewall:
IP Carrier Modem
IP Switch
VoIP Call
Other Corporate LAN Devices
(LAN-Corp)
VoIP Call
VoIP Phone Station With QoS
PC
VoIP Phone Stations With QoS
PC

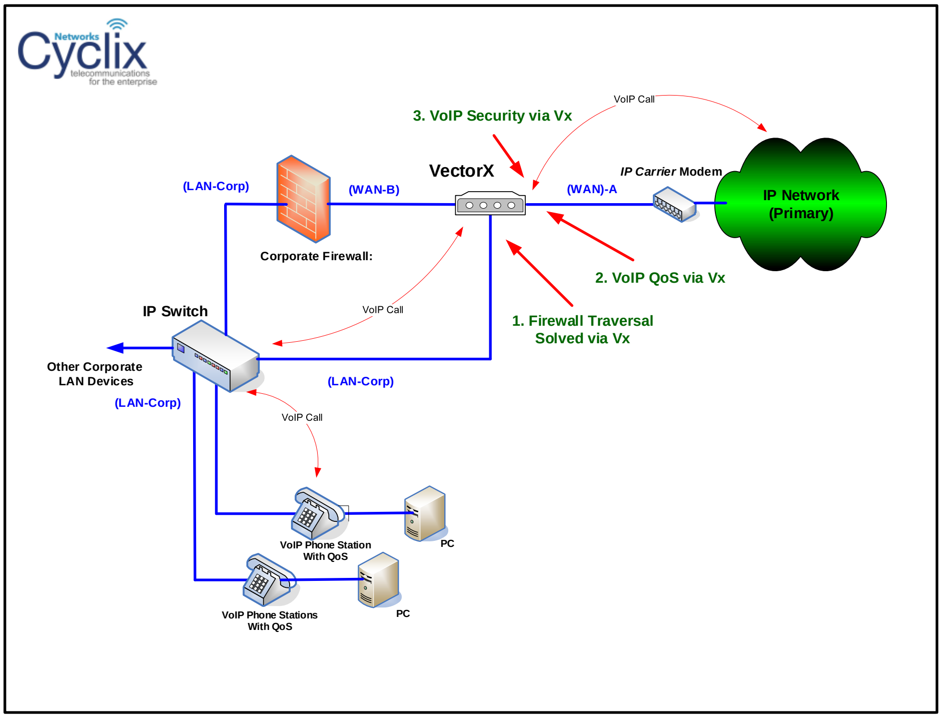
1. Call starts at phone
2. Traverses through the enterprise IP network switch
3. Traverses through the corporate firewall
4. Flows through the IP provider's broadband IP modem to the Internet

The problem surfaces in step 3 of the call route; i.e. the corporate firewall. VoIP signaling paths and VoIP voice path rules must be setup in the firewall to allow the VoIP traffic to flow correctly through this device, in both directions.

For most small and medium sized business users, this is a technical challenge that cannot be undertaken for the reason being that it requires intimate knowledge of the firewall, and how it should be configured for VoIP. Then, even if a solution is achieved, it often opens the enterprise to significant risks from hackers as essentially holes have to be opened up in the firewall in order to make it work for VoIP.

Cyclix solves this problem by introducing an Applications Layer Gateway (ALG) that is designed specifically to handle VoIP, and its special requirements. We call this ALG the VectorX™, or Vx™ for short. Here’s a diagram showing how Vx™ is used in a corporate LAN interfacing to the public internet.

Let’s examine how this call flows with the newly added Vx™ element…



1. Call starts at phone
2. Call traverses through the enterprise IP network switch
3. Call traverses through the Vx™ ALG
4. Call flows through the IP provider’s broadband IP modem to the Internet

With this new model we now flow through the Vx™, and so completely sidestep the client’s problematic firewall. Further, the Vx™ comes preconfigured for VoIP so there’s nothing the client needs to configure. It is completely plug-and-play.

We have solved the firewall issue by simply going around the problematic device, and adding in an element better suited to handle VoIP traffic.

Quality of Service

Next let’s look at the Quality of Service issues and solutions offered by adding the Vx™ to our network. When the Vx™ sees VoIP protocols, it knows it’s going to work on them, and do something special with them.

With Vx™ VoIP voice streams are given priority over the remaining bulk traffic, such as email, video and file transfers. Priority is accomplished by reserving bandwidth for the voice traffic so that there is always spare bandwidth for the voice, even if it means slowing down the bulk non-real-time traffic.

Handling traffic in this way assures voice streams remain clear, crisp, and uninterrupted, even during heavy call and bulk traffic load scenarios. So, voice with Vx™ always comes first, and *always* sounds good.

Security

Lastly, the other major benefit of introducing Vx™, either through Tangent™ with our SIP-Trunking products, or through our managed services Business-Connect™ product, is security. Vx™ knows where the Cyclix switching points are in the cloud, and uses that information to discriminate between valid VoIP signaling end-points and fraudulent signaling points.

Any other point outside of that set of validated signaling points is ignored. This results in exceptional VoIP security for the client, as the Vx™ sheds the hackers and criminals trying to take control of the client’s VoIP infrastructure.

VoIP security is a huge industry problem right now, with most VoIP carriers doing little or nothing to combat it. For more on VoIP security, and how Cyclix thwarts VoIP hackers attempting to steal your company’s minutes, see our other article titled “Cyclix Networks VoIP Fraud Prevention”.

Monitoring with EchoTest™

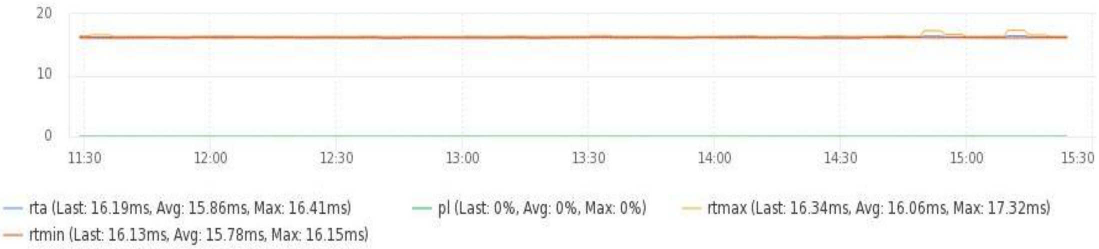
Last but not least is the monitoring of the broadband circuit that connects your VoIP infrastructure to the Internet, and your VoIP carrier. If this last mile circuit fails then all else described prior in the article is irrelevant, as the service is down.

So, to assure the basic integrity of the broadband last mile, Cyclix Networks has introduced EchoTest™. EchoTest™ is a service offered with its VoIP products that runs a circuit validation test on the connecting broadband vendors last-mile IP connection to the customer premises.

The test is able to determine the following characteristics of the circuit:

- **Service status—**is the broadband circuit in service or not
- **Network Delays—**the test will determine minimum, maximum, and average delays times for the circuit under test
- **Packet Loss—**the test will be able to determine when the broadband circuit has lost packets, and at what time, the loss occurred.

Let’s look at some EchoTest™ sample diagrams to better understand the power of this tool. Below we have what can best be termed a perfect IP connection to the internet.



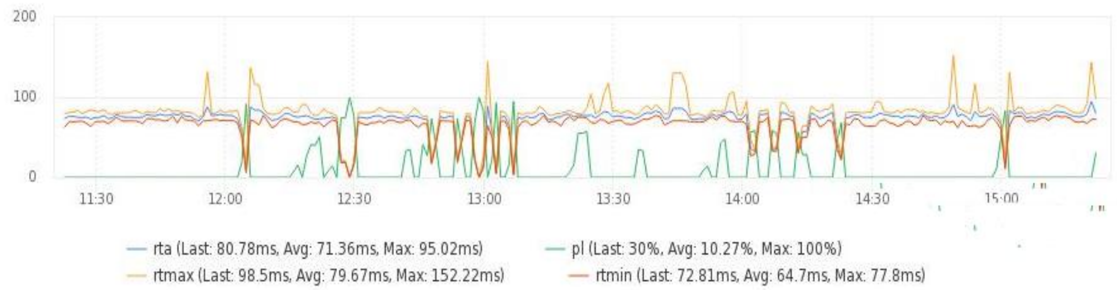
Echo-Test™: an error free broad-band connection

We see the following for this monitored circuit on this account…

- **Packet-Loss (PL)**= ~0 (i.e. a perfect connection to the internet)
- **Packet Delays**= The delays are low, and the Min, Max, and Avg are almost all the same as the circuit is so inherently stable.

So, in summary, the example shows a picture-perfect circuit for VoIP services to run over. Calls working in this sort of environment will be crystal clear and uninterrupted. Note that this particular test was taken from a client using a fiber connection to the premises.

Next let’s look at a problematic IP circuit being used by a Cyclix VoIP account…



Echo-Test™: an error ridden broad-band connection

In this example we see the following for this monitored circuit…

- **Packet-Loss (PL: bottom green line)—** continuous packet loss events, averaging a very high 10% over time
- **Packet Delays—**
  - For starters, the average delays are very high at close to 100 msecs
  - Max and Min delays are all over the board as a result of the heavy packet loss.
  - The wide variance in packet delays will usher in jitter (i.e. the uneven flow of voice packets), further degrading the voice quality

So, for this test, short of the circuit being completely down, it doesn't get much worse. Calls on this broadband circuit will sound choppy at best, and at worst will simply drop, as VoIP protocol will be violated from packet loss.

One interesting note here is this example taken from a cable broad-band deployment. Granted, this is an extreme case of poor performance. Most broad-band cable installations look much better than this. But one will likely never see this sort of poor performance with a fiber last-mile connection.

So, in review, by adding the Vector X™ element to the customer premises network we achieve the following:

1. **Firewall Traversal**

   Vx™ offers an alternate path on the customers LAN out to the Internet (WAN) thereby resolving the corporate firewall/VoIP compatibility issue.

2. **Quality of Service (QoS)**

   Vx™, with its VoIP Applications Layer Gateway, gives voice streams priority over non-voice IP traffic allowing VoIP and bulk IP transport to reside on the same broadband circuit, lowering network costs, and simultaneously providing for clean, clear phones calls at all times.

3. **Security**

   Vx™ has the ability to discriminate between valid Cyclix Networks signaling points and fraudulent signaling points. This gives the client very strong protection at the customer premises. This unique Cyclix Networks offering is unmatched by other VoIP carriers.

4. **Circuit Monitoring**

   Vx™ gives us a test point we can access remotely and use to gain insight into client's broad-band circuit quality, and suitability for VoIP transport.

VoIP users must realize that VoIP is a special service on an IP network that needs to be handled differently from bulk IP traffic. Because VoIP is a real-time service it must have an on-premises device managing and prioritizing it over other enterprise IP traffic. Hosted VoIP Carriers simply have no way to do that, and so choose to ignore the issue.

But with Vx™ these issues are all resolved at the customer premises. That, coupled with the other back-office VoIP services offered by Cyclix Networks, results in a VoIP service that finally realizes the true potential of VoIP for the enterprise; i.e. clear, uninterrupted, non-stop, secure calling, 24 hours a day, 365 days a year.

For further technical information, please contact sales at Cyclix Networks:

- 603-273-9292 opt 2
- sales@cyclixnet.com
- www.cyclixnet.com