NETEQUALIZER

WHITE PAPER

Hidden Nodes:
A Real Solution to a Virtual Problem

For years, our wireless Internet Service Provider customers (WISPs) have come to us to resolve their Hidden Node Problems. In this briefing, we discuss the Hidden Node Problem, and how it the NetEqualizer resolves this issue.

Of the numerous growing pains that can accompany the expansion of a wireless network, the issue of hidden nodes is one of the most difficult problems to solve. Despite best efforts, the communication breakdown between nodes can wreak havoc on a network, often leading to sub par performance and unhappy users. Many times, the cost of potential solutions appears to outweigh the benefits of expansion, which in some cases may not be a choice, but a necessity. Yet, hidden nodes are a problem that must be addressed and ultimately solved if a wireless network is to achieve successful growth and development.

Of the numerous growing pains that can accompany the expansion of a wireless network, the issue of Hidden Nodes is one of the most difficult problems to solve.

How Do Nodes Communicate?

First, we need to define what a "node" is. Nodes are defined as any computer or device that is within a network. In this white paper, the term "user" will refer to the individual or group utilizing these computers or devices and could effectively be interchanged with the term "node". In addition, the term "talker" will at times be used to refer to nodes that are sending data.

Now, let's move onto our discussion of Hidden Nodes. An 802.11 wireless network in a normal, simple configuration consists of a central access point (AP) and one or more remote users – which are the individuals utilizing the computers and devices that constitute a node, as shown in Figure 1 below.

Wireless transmission technology is such that if more than one remote user transmits data back to the AP at the same time, it is difficult for the AP to distinguish between the two talkers. When the forefathers of 802.11 first designed the protocols for how a wireless network should prevent this problem, they assumed that all users and nodes would be in close proximity to the access point and could actually hear each other's transmissions.

For example, say node A and node B are wireless laptops in an office building with one access point. Node A starts sending data to the access point at the same moment as node B. By design, node A is smart enough to listen at the exact moment it is sending data in order to ensure that it has the airwaves free and clear. If it hears some other talker at the same time, it may back off, or, in other cases, node B may be the one to back off, as shown in Figure 1 at right.

Figure 1: How Nodes Communicate with the Access Point

Node A and Node B start sending data to the Access Point at the same time. As Node B hears Node A talking, it backs off and waits to send its data.

The mechanism used to determine the back off order is similar to right of way rules at a four-way stop. These rules of etiquette are followed to prevent a crash and allow each node to send its data unimpeded. Thus, 802.11 is designed with a set of courtesies such that if one node hears another node talking, it backs off, going silent as to reduce the chaos of multiple transmissions at the same time. This is true for every node in the network.

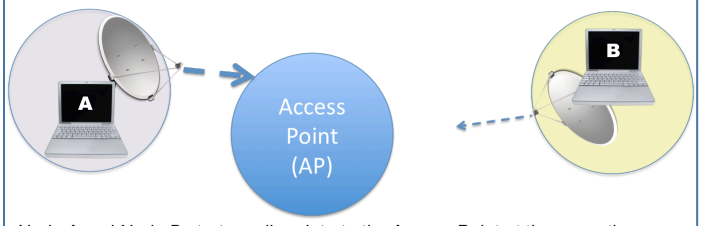
What Causes a Hidden Node?

This technology worked fine until directional antennas were invented and attached to remote nodes, which allowed users to be farther away from an access point and still send and receive transmissions. This technology is widely available and fairly inexpensive, and so has been adapted by many WISPs to extend Internet service across a community.

The impact of these directional antennas, and the longer distances it allows users to be from access points, is that individual nodes are often unable to hear each other. Since their antennas are directed back to a central location, as the individual nodes get farther away from the central AP, they also become farther apart from each other. This made it more difficult for the nodes to communicate. Think of a group of people talking while they stand around in an ever-expanding circle. As the circle expands away from the center, people get farther apart, making it harder for them to communicate.

Since it's not practical to have each node point a directional antenna at all of the other nodes, the result is that the nodes don't acknowledge one another and subsequently don't back off to let others in. When nodes compete to reach the access point at the same time, typically those with the strongest signals, which are generally closest to the AP, win out, leaving the weaker-signaled nodes helpless and unable to communicate with the access point, essentially becoming a "hidden node". This is shown in Figure 2 at right.

Figure 2: Node B becomes a Hidden Node



Node A and Node B start sending data to the Access Point at the same time. As Node A and Node B cannot hear each other talking, they do NOT back off. As Node A is closer to the AP, Node A has a stronger signal and wins. Node B is a Hidden Node.

When a network with hidden nodes reaches capacity, it is usually due to circumstances such as this, where nodes with stronger signals steal the airwaves and crowd out nodes with weaker signals. If the nodes with the stronger signals continue to talk constantly, the weaker nodes can be locked out indefinitely, leaving certain users without access to the network.

The degradation of the hidden node problem varies with time of day, as well as with who is talking at any moment. As a result, the problem is not in one place for long, so it is not easily remedied by a quick mechanical fix. But, fortunately, there is a solution.

How does the NetEqualizer Solve the Hidden Node Issue?

The NetEqualizer solution works by taking advantage of the natural inclination of Internet connections to back off when artificially restrained. The NetEqualizer method is solves the problem using ingrained 802.11 technology.

The key to making this happen over 802.11 relies on the fact that if you slow a stream to the Internet down, the application at the source will back off and also slow down. The NetEqualizer implements this without any changes to the 802.11 protocol, since the throttling is actually done independent of the radio. The throttling of heavy streams happens between the AP and the connection to the Internet.

> *"NetEqualizer will adjust offending flows by adding latency, forcing them to back off and allow potentially hidden nodes to establish communications – thus eliminating any disruption."*
>
> Art Reisman, CTO, APconnections

Radio manufacturers try to solve the hidden node issue with different schemes in the RF spectrum. This usually involves a proprietary polling or timeshare algorithm.

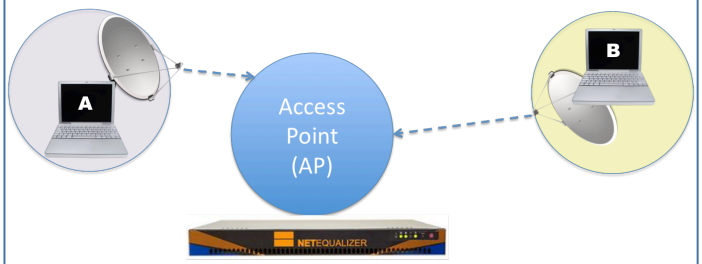
A NetEqualizer is placed between the Access Point and it's connection to the Internet. The NetEqualizer is then configured

to kick into gear when the upper limit of the Access Point is reached. We recommend using busy hour observation to determine the peak capacity of an Access Point.

Once configured, the NetEqualizer constantly measures the total aggregate bandwidth traversing the AP. If it senses the upper limit is being reached, the NetEqualizer will then isolate dominating flows, encouraging them to back off.

In our example, shown in Figure 3, when the NetEqualizer recognizes that the AP is constrained, it shapes Node A's traffic, which gives Node B time on the network. Node B traffic flows to and from the AP. Node B is no longer a Hidden Node. Node A's traffic is still flowing; only Node A's *dominating* flows have been shaped to ease congestion. Both Node A and Node B now have traffic flowing on the network. The Hidden Node problem is resolved.

Figure 3: NetEqualizer Solves the Hidden Node Issue



Node A and Node B start sending data to the Access Point at the same time. As Node A and Node B cannot hear each other talking, they do NOT back off. The NetEqualizer shapes Node A's traffic, which gives Node B time on the network. Node B traffic flows to and from the AP. Node B is no longer a Hidden Node.

How does the NetEqualizer Shape Traffic?

Each connection between a user on your network and the Internet constitutes a traffic flow. Flows vary widely from short dynamic bursts, which occur, for example, when searching a small web site, to large persistent flows, as when performing peer-to-peer file sharing or downloading a large file. By keeping track of every flow going through the AP, the NetEqualizer can make a determination of which ones are getting an unequal share of bandwidth and thus crowding out flows from weaker nodes.

NetEqualizer determines dominating flows from normal ones by taking the following questions into consideration:

- How persistent is the flow?
- How many active flows are there?
- How long has the flow been active?
- How much total congestion is currently on the trunk?
- How much bandwidth is the flow using relative to the link size?

If you have additional questions, please feel free to contact us via email: sales@apconnections.net or call us at 303.997.1300 x103

Once the answers to these questions are known, NetEqualizer will automatically adjust dominating flows by adding latency, forcing them to back off and allow potentially hidden nodes to establish communications – thus eliminating any disruption. Nodes with stronger signals that are closer to the access point will no longer have the advantage over users based farther away. The Hidden Node Problem is resolved.

About APconnections, Inc.

APconnections is an innovation-driven technology company that delivers best-in-class network traffic management solutions to give our customers be networks, with zero maintenance, at the best prices. We specialize in turnkey bandwidth shaping and intrusion prevention system (IPS) appliances. APconnections is based in Lafayette, Colorado, USA. We released our first commercial offering in July 2003, and since then thousands of customers all over the world have put our products into service. Today, our flexible and scalable solutions can be found in many types of public and private organizations of all sizes across the globe, including: Fortune 500 companies, major universities, K-12 schools, and Internet Providers on six (6) continents.

