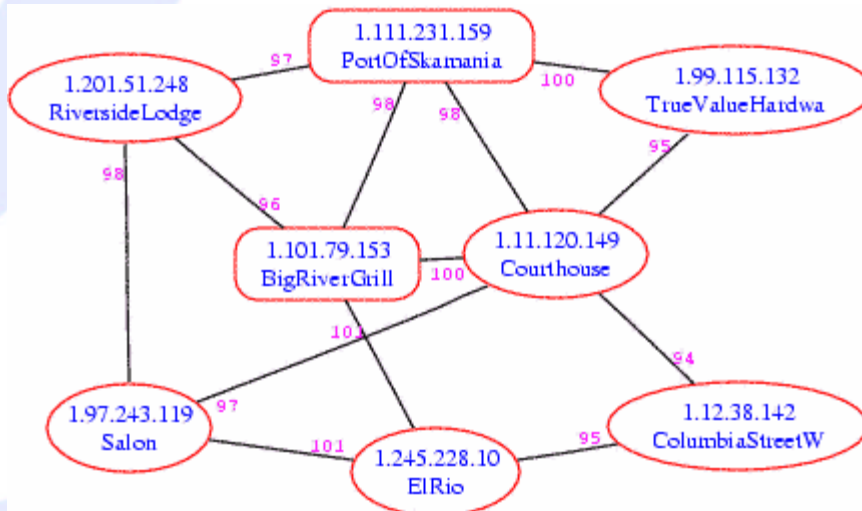




Qorvus Qnode™ Wireless Mesh Systems- FAQ's and fiction

Qorvus Systems, a leader in the design and implementation of outdoor wireless equipment, has developed the **Qnode™**, an efficient, affordable, and rugged indoor / outdoor WiFi-compatible wireless mesh router and switch, that allows networking professionals to plan, rollout, and easily scale a wireless local-area or wide-area hot-spot network for use in fixed or mobile wireless applications. The **Qcode™** firmware running in the **Qnode™** is based on highly-regarded open-source networking and wireless driver software written by the National Institute of Standards and Technology, the Linux open-source community, and the technical staff at Qorvus Systems. To aid in transitioning the original code-base from an experimental platform to a truly viable commercial product, Qorvus has streamlined and enhanced the open source code to include a variety of important functions such as SNMP, QoS, an embedded web-server with real-time RSSI and link-quality tools for initial setup and management, and a wide variety of stability and reliability improvements.

Many wireless networking professionals are already familiar with the concept of wireless mesh networking. Briefly, it's a local or wide-area wireless deployment and routing approach that serves to extend wireless access throughout a large area, up to many square miles in size, without either expensive tower-mounted point-to-multi-point equipment, or individually cabled Ethernet data backhaul connections to each distributed access point. Instead, the signals hop to and from the client's desktop or laptop (or industrial sensors, attached hi-res IP video cameras, etc) to the nearest mesh-enabled access point, securely tunnel through the mesh to the remote gateway which, in turn, routes the signal out to the internet (or sometimes to local content servers). In so doing, the signal may traverse 2 or 3 other roof or pole-mounted mesh-enabled access points, before reaching the gateway node (1.101.79.153 in the installation below).



It's apparent that a wireless mesh approach can have significant advantages over traditional wireless deployment methods. The most obvious is a tremendous savings in cost and effort, realized by eliminating the need for high tower mounted access points, or separate hardwired or wireless backhaul to each low-level access point.



The self-organizing and redundant nature of a properly-designed mesh system also provides real benefits of faster installation, increased uptime and overall system reliability.

However, some networking professionals have been reluctant to deploy a system based on wireless mesh, because of concerns that have now become a part of what could be referred to as "Mesh Folklore." Here are some of the questions and comments we hear most often:

Question: Wireless mesh systems use client radios to repeat their signals. If a critically placed client disconnects, won't the mesh quit working for all downstream users?

Answer: While it's possible to implement a mesh topology using client radios, it's poor practice in anything other than, perhaps, an experimental or itinerant field situation. The **Qnode™** mesh system uses stand-alone mesh nodes, that provide all necessary infrastructure without depending on any client-side radios or services.

Question: Don't wireless mesh systems require all client radios to operate in ad-hoc (peer-to-peer) mode?

Answer: This was true in some of the early mesh experiments, and still seems reasonable because the mesh nodes communicate among each other in a peer-to-peer topology. Nevertheless, the client-access radios within the Qorvus mesh nodes operate in host infrastructure mode and with infrastructure performance, meaning that standard client association and management tools can be used, as they would in any ordinary wireless LAN or hotspot installation.

Question: Aren't mesh systems inherently insecure when compared a standard wired or wireless deployment?

Answer: The **Qnode™** mesh system can be configured to utilize 2048 bit certificated encryption and encrypted PtP tunneling between stand-alone mesh nodes and the gateway. This traffic is at least as secure as VPN traffic over the public internet. And client-to-node traffic can use the standard VPN clients included in Microsoft Windows XP and Vista.

Question: Don't mesh systems suffer from poor performance?

Answer: A properly designed and deployed mesh-based system performs as well as a conventionally designed system, and with reduced installation costs, management hassle, collision domain and hidden-node problems. For example, even using standard 802.11b radios and a standard business dsl connection at the gateway, the Qorvus mesh systems readily achieve net user data rates of 1 Mb/s and raw data rates of up to 3 Mb/s, even after several hops. And in a recent video surveillance installation using Atheros 5 Ghz and 900 Mhz OFDM radios, net sustained data rates of over 10 mb/s are being achieved at the gateway node. This mesh is delivering about 65 Gigabytes/day of compressed IP video data from five



downstream perimeter IP surveillance cameras to the gateway attached server. And this performance will only get better, as faster radios and better driver technology (currently under development) come on line.

Question: How do you manage these mesh nodes once they are in place? Do you support e.g. Openview or Nagios management, etc?

Answer: While each box can currently be managed individually using ssh, web-based tools and SNMP, a comprehensive web-based management system has been developed, which allows complete monitoring of individual mesh nodes and the mesh as a whole. Some of the features include automated email alarms for each node, Radius and Automac authentication, VPN security, data compression, host and port mapping, variable firewall and bandwidth throttling on a per user-class basis, remote CPU, voltage, and temperature monitoring, graphic representation of routing and association tables, bandwidth use per hour, etc. etc.

Question: Aren't mesh systems more expensive because they require two radios and two antennas- a directional one for backhaul, and an omni for client access?

Answer: While we generally recommend the use of multiple radios for mesh data backhaul and distribution, acceptable performance can often be obtained while using just one radio with an inexpensive omni, in a data-compression & store-and-forward modality. Even using dual radios for best performance, the costs compare very favorably to standard enterprise-grade access points, and with the much easier installation, dramatically enhanced functionality, and greater flexibility that our mesh technology affords.

If the idea of saving up to 50% of your up-front network engineering and installation costs appeals to you, please contact us at 800.757.1571 or via email at sales@qorvus.com

Further information is also available on the web at www.qorvus.com