Q: What type of network assessment would be appropriate for determining the stability of your current network infrastructure to support Wi-Fi connectivity?

Answer from Dwayne MacKenzie: Really what we look at when we are trying to understand your current infrastructure we do what we consider to be a performance assessment where we make sure there are adequate gigabit Ethernet connections for the APs and that you have adequate backbone bandwidth to support the number of users that you are going to have. We also do a security review to look at the security that exist on the network and leverage the existing security as much as possible. What we don’t want to do is create a Wi-Fi network and then create separate security policies for the Wi-Fi creating a situation where we would then need to manage two, three or four different systems. So we try to leverage as much as we can from the existing network and security to support the Wi-Fi.

Q: Can a Cisco or Linksys wireless router/access point be hooked up to your internal network and be totally secured, especially if running open Wi-Fi? Can you run open Wi-Fi with Juniper and have it be secured?

Answer from Bruce Alexander: The answer to the second question is easier. Yes, you can run open access for guests. By open access I’m assuming you mean anyone can get on. If that happening the open access meaning the guest access obviously is not secure because anybody can get on. But what you can do is segment that traffic in VLAN and out the firewall so it is securely separated from the corporate traffic. That is very easy to do.

The first question, can you take a Linksks or Cisco? I’m not exactly sure what that means. No you cannot tie a Linksks or Cisco device into the Juniper wireless. No vendor does that – that is a fact. Full functionality is not going to happen across any vender.

Regarding Linksks you can’t even put two Linksks on the same network and have them actively roam and perform all the features between them. Linksks is designed for the Home market. The home market is drastically different in terms of security, authentication, and advanced features from the commercial market whether it be Cisco and Linksks or NETGEAR and Aruba or Juniper and D-Link. The products and features are drastically different between the home market and the corporate market.

Q: What are the steps in your authentication process? Do you need to just ask for the password, or need special tokens to be able to be on the wireless network?

Answer from Dwayne MacKenzie: The answer is... it depends. The flexibility of the solution really comes down to: if you want authenticated access you can use Active Directory credentials or you can use pre-shared keys. It is very flexible. It is possible to do two (2) factor authentication as well. The access to the wireless network is based on the ability of the device and what the device can do rather than what the wireless network can do.

Answer from Bruce Alexander: Not only can you do all those things you can set them up so that the guest access has one type of authentication, the contractor access has a different type of authentication and authorization of policies, the user has a different set and IT has a different set. You can mix and match based on user, based on SSID, based on type of device – hey that’s a IOS device so I’m not letting it on my corporate network but it can be a guest. All those things come into play and we can drive down deep and have a huge cross matrix of what’s available for what type, who, etc.
Q: What are the first steps to take if you’re in the beginning stages of installing wireless into a small school?

Answer from Dwayne MacKenzie: The first steps are what we covered in our 7 considerations. Really to look at your requirements for Wi-Fi and what your plans are for access needed over the next 3 – 5 years. Then develop a plan based around that as well as looking at the performance of your exiting wired network and the security that is in place and what changes will need to be made or if it will support the Wi-Fi that you want to do.

Q: What is Wi-Fi’s impact on VLANs of the wired network and what is Best Practices?

Answer from Dwayne MacKenzie: The good thing is that the network is designed with existing VLANs where you are segmenting traffic based on the user’s identity or the type of user or even physical location. You can actually utilize those in the Wi-Fi arena so that you can actually have devices that are in a specific department access the same VLAN that they would if they were on a wired machine.

Best Practices around that truly are to segment VLANs based on user types, and as Bruce has mentioned, a big one is guests. You really want to treat guests differently than you treat your authenticated or authorized users. So the Best Practice there is to create a VLAN design that incorporates into the security of your wired network and even sometimes into your perimeter. The key is that if we can integrate those together we are only managing security policies once. We do not actually have to deal with Wi-Fi VLANs and security in the Wi-Fi and then infrastructure or wired VLANs and security and then even different policies on the perimeter where we have different types of access and security requirements.

Q: How does Juniper equipment compare to the Cisco Aironet line?

Answer from Brue Alexander: There are 3 primary components in wireless. Access Points, Management – I group management with lots of different things – and the Control functions. Sometimes the controllers and management is tied together. In terms of differences on APs, at Juniper we have fewer models - we have an outdoor AP, a lower end AP, and Juniper has an AP that equals or excels the Cisco “top of the line” 3600 AP. From an AP point of view across the board we are on par with Cisco. As far as controllers we have the virtual controller that now allows you to put it virtually into the network. Our controller does not require traffic to flow through it for data. That’s the primary architectural difference between Cisco and Juniper controllers. And management platform, not sure what Cisco is doing currently. Juniper is integrating management so that we can manage our infrastructure devices-switches, security firewalls, etc with the same product line and platform as the wireless.

So in terms of what the difference is between Cisco and Juniper I would ask you to compare:
1. The Specification - when you get down and deep you can look at many different things
2. Compare the price tags
3. Look at the cost of ownership over 5 years including support and maintenance.

These are the three things you want to examine.