How to set up a network

Service provider takeaway: Network consultants and value-added resellers can optimize their customers' network reliability and performance by adhering to fundamental best practices during network setup.

With virtually every device and software application in the modern business world requiring network connectivity, ensuring a sound network is of prime importance. Although the industry has done a great job of making networking mostly a matter of "plug-and-play," this simplicity could result in network performance and reliability problems. These problems can be avoided, however, by following fundamental best practices when you set up the network.

1. **Plan ahead!**

   Before you begin configuring your customer's routers and switches, get a rough idea of how many devices need IP addresses on the network, and then multiply that number by two or three. As time goes on, your customer will connect more and more devices to the network, and the last thing you want is for them to run out of capacity on the subnet.

   For a company LAN that needs to support typical business usage, avoid using anything larger than a 24-bit subnet for devices. A 24-bit subnet can support 254 devices on the same broadcast domain, which could result in a lot of broadcast packets that decrease performance. If the customer has more than 254 devices, consider configuring VLANs to segment the network into logical groupings. The groupings could be by business unit (for example, sales, management or engineering) or by device technology (voice or data). This not only confines broadcast packets, but allows for tighter control of security while providing room to grow. You can create port-based VLANs on most medium-grade switches and up, and many of these devices also support VLAN tagging using 802.1Q for more advanced configurations.

2. **Use conventions**

   The more networks you set up the same way, the easier they will be to manage and troubleshoot. Here are a few pointers to help you create a template.

   - Use a valid C-class network. 192.168.x.0 /24 (255.255.255.0) is a valid network according to networking conventions and standards. Although you can use 10.0.0.0 /24 subnets and the like for the LAN, it is technically incorrect.

   - Set up DHCP to start and end on a certain range of IP addresses. Unless you have a unique situation, have the DHCP lease address range between .100 and .254. This way if you ever need to set up a static device, there is no question it needs to go below .100.

- Logically group static devices within a certain IP range. For example, set network-related devices in the .1 through .10 range. Put servers between .11 and .20, network printers between .21 and .30, etc. This way you can effectively add and find statically set devices on the network, without knowledge of the exact address.

- Use the same nontrivial passwords for administrative devices on a given network. It saves time and headache to be able to go to four completely different network devices and use the same username and password to log in. It saves time and headache. However, it should go without saying, different networks and different customers should absolutely have different passwords for the sake of security.

3. Configure DHCP to be resilient

Configure the network router to do DHCP as opposed to the server. The last thing you want is for the server to fail, and then have all your customer's users lose Internet connectivity after their DHCP lease expires. This way if the servers fail, workstations will still be able to utilize the network for other purposes.
A word of caution: Be sure to properly set the DNS IP addresses issued by DHCP to the network's Primary Domain Controller (PDC) if you are using a Microsoft Windows Domain. Due to Active Directory's heavy reliance on DNS, if a client workstation doesn't have the IP address of the PDC set as its primary DNS server, your customer will experience serious problems on the workstation, resulting in no end to user complaints.

4. Get rid of hubs

Old infrastructures may still have a hub sitting around here or there from back in the old days. In fact, I just visited a company this week that was still using a hub at the core of its network! Network switches are dirt cheap, and their performance-to-use ratio is infinitely better than their expired counterparts. That isn't to say go and buy the cheapest switch you can find -- the medium-grade switches provide more error-free operation and last longer.

5. Use a firewall

Many people argue that simply having a NAT-enabled router is a significant barrier against threats. Although it does provide the ability to block out a fair number of attacks, it's a far cry from the comprehensive coverage a stateful firewall provides. Most routers have a firewall on them, but the functionality is disabled due to the extra management and configuration it requires. Although it may be a pain to configure and tweak as people report connectivity problems, a router firewall is much better than unnecessarily leaving the customer's network and data vulnerable to attack.

Network design and architecture is a very complicated practice, as every network has different requirements and demands that must be assessed and addressed. However, the above five tips on how to set up a network are applicable to virtually every business network as a starting point.