



Modernizing the Network

Wireless networks: Getting ahead of the demand _____	S2
Bandwidth hogs: What's on your network? _____	S3
Under attack: Network security trends _____	S4
The cloud: An extension of your network _____	S5
Future pipes: 4 networking technologies for the future _____	S6

Wireless networks: Getting ahead of the demand

What's the fastest-growing traffic segment of wireless networks? The answer for a large majority of organizations and agencies is traffic from wireless devices, and that growth is showing no signs of slowing down, says one expert. "It's kind of like trying to stop the tide," said Bob Laliberte, a senior analyst at Enterprise Strategy Group. "You either adapt or get run over by it."

The growth of wireless device traffic comes from inside and outside of organizations. Some of the traffic comes from organizations and agencies extensively deploying their own wireless devices such as tablets and smart phones. Last fall, for instance, the Veterans Affairs Department announced it was acquiring up to 100,000 tablets including iPads as well as those that run on Android and Windows operating systems, and even the White House is looking to add a Wi-Fi network, which would encompass 60 buildings and several outdoor areas.

Employee-owned devices contribute, too. Some of the wireless usage is sanctioned as part of a bring-your-own-device trend, a policy that allows end users to access an organization's data and network using a personal device. For instance, a recent Gartner Inc. study — "User Survey Analysis: Impact of Mobile Devices on Network and Data Center Infrastructure" — found that, of the organizations surveyed, 32 percent said they support employee-owned smart phones, 37 percent support employees' tablets, and 44 percent support their laptops. The biggest change: The wireless network has gone from being a secondary network to a primary one for many users.

However, there's also a sizable portion of the traffic that comes from employees accessing the network on their own without IT's knowledge or approval. One recent Forrester study found that 40 percent of Generation Y workers said they will bring their own devices to work whether IT supports them or not.

Filling in the holes

Organizations that want to provide stable, reliable wireless service might think that the key to doing so is simply adding access points, but this strategy doesn't work for every organization or every wireless network. The first step that all agencies should take is an assessment that identifies the type of traffic going over the wireless network. Are users accessing e-mail and software as a service? Are they using their devices for virtual desktop access? Are they looking to implement unified communications? The answers, say experts, will dictate the equipment, security and management tools that will be required for success. And some organizations might do an assessment and realize that they don't need as much wireless coverage as they thought so they can focus on guest access.

Once agencies can predict growth based on current usage patterns, they might want to reassess the wireless technology that is in place. For most, the current installed technology is based on the 802.11n standard, using two spatial streams for a theoretical throughput of 300 megabits/sec — 150 megabits/sec of throughput per stream. But just because the technology is mature doesn't mean that technologists aren't able to get more out of the standard. Today, there are several vendors that market three-stream access points that provide up to 450 megabits/sec throughput and with good results, said Craig Mathias, principal analyst at Farpoint Group, an advisory firm specializing in wireless and mobile technologies. "We've seen up to 100 percent improvement [in capacity] for three-stream versus two-stream access points," he said.

In addition to wireless equipment, Mathias said it is crucial for every organization to make sure that the wired network can handle the traffic coming in from wireless networks. "The wired network is a major component of wireless success that the majority of people just don't think about," he said. "The systems are interconnected components, and you always have to think about the weakest link of the chain." ▲

Bandwidth hogs: What's on your network?

Data growth, like death and taxes, is a given. And data growth, as any network administrator will tell you, comes with an increased need for bandwidth.

According to the Cisco Visual Networking Index: Forecast and Methodology, 2011-2016, “annual global IP traffic will surpass the zettabyte threshold (1.3 zettabytes) by the end of 2016. In 2016, global IP traffic will reach 1.3 zettabytes per year or 109.5 exabytes per month.” Overall, IP traffic was expected to grow at a compound annual growth rate of 29 percent from 2011 to 2016. A growing amount of that traffic is coming from non-PC devices, with as much as 31 percent of traffic originating from non-PC devices by 2016. Meanwhile, by the same year, traffic from wireless devices will exceed traffic coming from wired devices, with mobile and Wi-Fi devices accounting for a whopping 61 percent of all IP traffic.

There are several factors pushing this growth. One driver is the bring-your-own-device trend, which allows end users to access an organization’s data and network using a personal device, and it’s a trend that’s catching on, according to a recent Gartner study, “User Survey Analysis: Impact of Mobile Devices on Network and Data Center Infrastructure.” According to the study, 90 percent of enterprises have already deployed mobile devices, and they are supporting their employees’ devices, too.

Another major driver in IP growth, at least for some, might be unified communications (UC). “From our data...the number of remote users and those working from home has increased 33 percent,” said Andre Kindness, an analyst at Forrester Research. “The knee-jerk reaction is, ‘Let’s get a bigger box,’ but the problem is most people don’t have the money to do it.” There are options, however, that can help network administrators handle the increased bandwidth load.

Making it work

A better option, Kindness said, is for network administrators to focus on monitoring and shaping traffic to better use the bandwidth they already have.

It’s fairly easy to prioritize UC activities such as voice, streaming video and virtual desktop infrastructure traffic — all of which are highly sensitive to latency issues — and let less critical traffic such as e-mail or Web activity move as bandwidth allows, said Jim Frey, managing research director at Enterprise Management Associates. “E-mail traffic can wait five or eight seconds,” he said.

That requires network professionals to make better use of networking tools. Although that might sound like common sense, only a small percentage of network professionals are using network tools even on a limited basis. That is mostly due to the fact that network professionals don’t always understand what’s out there or how to use what they already own, according to Kindness. “Ten years ago, you needed multiple tools, but now monitoring has [morphed] from fault-finding to analytics.” And network professionals need to catch up, he said.

Because network refreshes are also a given, some forward-thinking network managers are taking a different path during a planned upgrade, overhauling their networks and flattening them from three-tier to two-tier Layer 2 networks. There are two big advantages to that strategy. “You get better throughput and it’s a simpler architecture, so you buy fewer boxes and the boxes you do have get used more fully,” Frey said.

The challenge with this strategy, however, is that with flatter network fabrics it often makes sense to stick with one vendor. The time to do that is during a consolidation project when everything is being swapped out, Frey said. “Consolidation activities tend to have very strong cost savings over time so they are usually very easy to justify,” he said. ▲

Under attack: Network security trends

No network is infallible. Case in point: In May, Anonymous announced that it had successfully hacked a U.S. Justice Department Web server, one that housed data for the Bureau of Justice Statistics. The loss was significant: 1.7G of data, all of which was available for download on The Pirate Bay. The rogue group was pleased with its score. “Within the booty you may find lots of shiny things such as internal e-mails and the entire database dump,” it posted on its website.

If the Justice Department’s server was vulnerable, it stands to reason that every entity that produces, analyzes and stores public or private data is vulnerable, too. Data is the key, according to Trustwave’s 2012 Global Security Report. Today, customer records are the No. 1 target for attackers, with 89 percent of all investigated breaches being related to data theft. The stolen information includes “payment card data, personally identifiable information and other records, such as e-mail addresses,” according to the report. Another growing target: theft of trade secrets.

Starting fresh, starting safe

Although there is no perfect network, a network refresh does provide the opportunity to increase the level of security in a particular IT environment. It is especially important as other resources such as cloud-based servers and virtualized servers become part of the overall landscape.

One of the biggest adjustments that IT managers and employees need to make is changing the way they think about network security, said Jon Oltsik, a senior principal analyst at IT advisory firm Enterprise Strategy Group. “Now you have to think about ingress and egress,” he said. “Typically, we only looked at traffic coming into the network, but now you have to think about both internal and external traffic. We have to inspect the traffic going out, too.”

That requires higher throughput and processing devices on the network. Next-generation firewalls that are

contextually aware and able to triangulate traffic and users to enforce policies are a good addition to the infrastructure, Oltsik said. In addition, full packet capture on the network allows administrators to view what’s going over the network, who the source is and what the destination IP address is. “This gives administrators a much deeper understanding of the network,” he said.

Another change to network security is that the focus on security is moving up the stack, said Jim Frey, managing research director at Enterprise Management Associates. Firewalls that work at the application layer instead of the network layer are taking on more importance. “The better you can lock down and track the movement of data, the better off you are,” he said. That is because threats are coming in more frequently in the upper layer of the stack. The most insidious ones are high in the application layer, he said. Although Web- and application-layer threats aren’t new, protecting the network at that level has taken on greater importance.

Finally, network administrators are looking to secure something that in the past was often out of their responsibilities: wireless devices and the wireless network. Smart phones in particular have vulnerabilities both from a user perspective — users fail to implement even the most basic security protections — and because they are often connected directly to the network via a Wi-Fi connection. Even Apple’s once impenetrable iPhone operating system has fallen victim to a malware attack. In July, a hacker uploaded what is being called the first malicious app to the Apple App Store. Called “Find and Call,” the Trojan app uploaded the user’s contacts to a remote server. And that is why security has to change, analysts say. As Frey explained: “It’s all about the weakest link in the chain.” ▲

The cloud: An extension of your network

There's a problem facing more and more network administrators every year, and it's something that's being mandated in the federal government and heralded as a powerful, money-saving tool. It's the cloud, and as it becomes more ubiquitous, the issues surrounding it will only become more pronounced.

And it's something that's sure to happen. Data bears this out. For instance, in the government sector, the deadline for identifying at least three services to migrate to cloud solutions passed in June. Meanwhile, the majority of defense and civilian agencies are ready or will soon be ready to move to the cloud, according to Deltek's "Federal Cloud Computing Services Outlook, 2012-2017." The problem, experts say, is that although the IT department as a whole might be ready to make the move, network administrators might need to do some work, said Andre Kindness, an analyst at Forrester Research.

"When it comes to the cloud, what I have found is that the networking team is about 18 to 24 months behind business units or those in the data center," he said.

The reason for the disconnect

The problem is twofold. First, although the cloud has caught on as business users and those in the data center use it to get their work done more quickly, they rarely consult with the networking team to make sure their new cloud services mesh well with the existing network. Meanwhile, although it's true that the cloud has always been part of the network, it's only recently that network administrators have started to think about control and integration. The combination creates a new wrinkle for network administrators, especially those who are modernizing the network, according to experts.

"If you have an application hosted on a site, you might need a point-to-point [virtual private network]," said Jon Oltsik, a senior principal analyst at IT advisory firm Enterprise Strategy Group. "You need to coordinate encryption keys. You might have to bring together an

authentication system. If you think about the cloud as an extension of the network, you have to treat it as such."

When you don't, user satisfaction suffers, turning the very thing that was supposed to increase productivity into something that impedes it, Forrester's Kindness said. Everything on the local-area network has to go across the wide-area network, he explained, but bandwidth differs wildly. The WAN's bandwidth is only a fraction of the LAN's, and users, even those in IT, don't think about that fact. "Then, when they are having a problem, they complain to the network team," Kindness said.

That might be rooted in a generational gap. The average networking professional is in his or her 40s, while application developers are in their 20s, according to Forrester. The two groups don't talk much, and when they do, they're not communicating effectively, Kindness said. That will have to change in order for organizations to get the most out of the cloud, he said. Network teams, for their part, need to start working on tracking and analysis. They also need to offload some of the manual processes that take up their day, using management programs to handle some of the repetitious tasks and one-offs that don't require real networking knowledge.

"When you automate even 5 percent of your management, you free up the human resources," Kindness said. "Engineers probably don't want to be typing things in and filling out spreadsheets. Instead of being bogged down on setting up infrastructure and doing config files for switches, they can become part of this proactive group using the cloud and finding solutions out there like WAN balancers and load optimizers to increase the user's satisfaction." ▲

Future pipes: 4 networking technologies for the future

What will the network look like tomorrow? Although the traffic itself probably won't change too much, the topology and tools that enable the network will be new and will require network administrators to educate themselves and their teams. Here are four network technologies and trends that everyone in IT will be hearing more about in the coming year and beyond.

OpenFlow: This open standard, which was developed at Stanford University, is being used to deploy innovative protocols in production networks, according to the Open Networking Foundation. It enables organizations to remove the control plane from the forwarding plane or the routers and bring it back and centralize it so they can easily partition and run different services, said Bob Laliberte, a senior analyst at Enterprise Strategy Group. "Companies like Google use it," he said. "The main reason to use OpenFlow is that it is an API that allows a switch to talk to a controller. An OpenFlow controller can help derive some of the more intelligent network functions. By adding this level of programmability into the switches, it allows the ability to scale an environment without having to deal with all the manual processes that usually accompany consolidating or scaling out a data center."

NetFlow: This network protocol, developed by Cisco Systems, has a big place in today's network and the future. At its core, NetFlow lets network administrators monitor all the different network sessions going on at any given time. Although the protocol isn't new, the fact that a wide variety of network management systems are designed specifically to harvest and analyze NetFlow records is. Another emerging trend: The use of tools designed to find security issues using NetFlow records.

5G Wi-Fi (802.11ac): The next step after 802.11n, which enjoys wide deployment, is backward-compatible so network administrators can deploy it today to support current and future devices. The main benefit of 802.11ac is speed, said Craig Mathias, principal analyst at Farpoint

Group, an advisory firm specializing in wireless and mobile technologies. The technology ups the amount of spectrum that we use in a channel. With 802.11n, there were 40 MHz channels. With 802.11ac, network managers will use 80 MHz and conceivably even 160 MHz channels.

"That's a lot of spectrum," Mathias said. "The initial performance that people are going to hear about is 1.3 gigabits/sec versus the upper [boundary] of 600 megabits/sec — or, practically speaking, 250 megabits/sec — in 802.11n. So we're going from [250 megabits] to 1.3 gigabits." In practical terms, 802.11ac is the first wireless standard to break the gigabit barrier, a fact that has been widely reported and anticipated.

Ultimately, it's not all about throughput, it's about capacity, and 802.11ac delivers, Mathias said. "It's not so much about giving you hundreds of megabits per second. It's more about getting a lot of users on the air with an incredibly diverse array of applications and data types."

Centralized network controls and out-of-band management: Network administrators will need greater control over all the networks in their organizations — wired and wireless — as well as disparate devices. Today's users are likely to have multiple devices and use them fluidly, moving from their desktop to their tablet PC to their smart phone in a matter of minutes. When they do that, they want access to their data, and they expect their experience to be the same no matter which device they are using, said Jon Oltsik, a senior principal analyst at IT advisory firm Enterprise Strategy Group.

Because of those trends, network administrators will need the ability to control and enable access across multiple devices and networks while at the same time enforcing network access policies at a more granular level, Oltsik said. ▲