Is Your **IT Infrastructure** Ready for Mobility?

IT departments have been unable to stop the proliferation and use of consumer devices in their enterprise environment, and tablets are the latest technology to challenge the corporate network. We’re already seeing consumers adopting tablets at an exponential rate. It’s only a matter of time before these consumers (who are also employees) drive the onslaught of tablets into the workplace. The presence of these consumer mobile devices in the corporate arena will only increase as more manufacturers bring their own tablets to market, driving greater competition, causing prices to drop, and the refinement of the technology to deliver high end-user satisfaction.

An increasing number of organisations feel that it’s necessary to support corporate applications on employee-owned devices, such as smartphones and tablets. Driven by employees who prefer to use their own smartphones or tablets for personal use, as well as for business, the decision to move in this direction will become ubiquitous in the next few years and will force many enterprises to support a variety of mobile platforms.

Fortunately, solutions exist to help organisations meet the requirements of the increasingly mobile workforce. In particular, 802.11n (Wi-Fi) enables optimal coverage, reliability and predictability across the corporate network infrastructure for data, voice, video and other mobility services vital to support mission-critical mobile applications and services. In many instances, connectivity includes mesh topology to support communication in emergency situations, outdoors or in harsh environments. At the corporate campus, appropriate media gateways and routing platforms can be installed to interconnect with IP PBX (telephone systems) and external networks. When designing wireless networks, keep in mind that they will need to support multiple user devices and operating systems.

In this report, we’ll discuss how organisations can effectively support an increasing number of personal mobile devices, review best practices to optimise corporate infrastructures to support these mobile devices and help organisations realise the benefits of enterprise mobility. This is all within the context of an infrastructure competency, a critical component of an enterprise mobility strategy.
Mobile: it’s how business is done

Employees are increasingly looking to stay connected while on the move. Over the past 12 months, there’s been a remarkable increase in the number of employees who think that mobile devices, especially smartphones and tablets, will increase in importance for advancing business productivity (according to the 2011 InformationWeek Mobile Device Management and Security Survey; see Figure 1 below). As these devices increase in importance for business, employees will require the same quality of access to the corporate network to maintain productivity regardless of whether they’re using a wired connection at their desk or a mobile connection on a wireless device.

If your employees don’t have high quality access to the network or have difficulty accessing corporate data and resources while on the move, you and your customers will likely witness a negative impact on business services. The inability to communicate via e-mail or connect to organisation’s data and resources can limit a mobile employee’s ability to address customer needs and enquiries in a timely manner, which will lead to poor customer satisfaction or worse, loss of customers and their business. As seen in Figure 2 below, employees have become accustomed to e-mailing and connecting to the corporate network from mobile devices. This is the way businesses operate today.

IT departments must prepare their wireless network infrastructures for tablets and other mobile devices. Basic connectivity isn’t enough. High levels of reliability and performance are critical when supporting a workforce on the move. To ensure this, protect these networks from interference and eliminate dead coverage zones. As more bandwidth-hungry applications and media content stream across the network to mobile devices, put in place mechanisms that ensure scalable delivery of video. Most importantly, use the latest security mechanisms and protocols to avoid and/ or mitigate threats that might compromise the network and sensitive corporate data.

**Figure 1: Mobile technology impact on productivity 2010 vs. 2011**

Thinking about the next 24 months, how critical a role will the following mobile technologies play in business productivity at your company?

<table>
<thead>
<tr>
<th>Mobile Device Type</th>
<th>2010</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphones</td>
<td>82%</td>
<td>89%</td>
</tr>
<tr>
<td>Tablets</td>
<td>36%</td>
<td>79%</td>
</tr>
<tr>
<td>Laptops</td>
<td>34%</td>
<td>53%</td>
</tr>
<tr>
<td>Kiosk-based Web access</td>
<td>24%</td>
<td>21%</td>
</tr>
<tr>
<td>Netbooks</td>
<td>22%</td>
<td>38%</td>
</tr>
</tbody>
</table>

Note: Percentages reflect a response of ‘increase significantly in importance’ or ‘increase somewhat in importance’
Base: 323 respondents in August 2011 and 307 in March 2010
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals

**Figure 2: Lack of access to mobile productivity activities: impact on employees**

If your users were to lose the capability to conduct the following mobile productivity activities, how great an impact would it have on them? Please use a scale of 1 to 5, where 1 is ‘they wouldn’t notice’ and 5 is ‘mass insurrection.’

<table>
<thead>
<tr>
<th>Mobile Productivity Activity</th>
<th>2010</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communicating information by e-mail</td>
<td>4.4</td>
<td>4.5</td>
</tr>
<tr>
<td>Making a remote connection</td>
<td>3.6</td>
<td>3.7</td>
</tr>
<tr>
<td>Storing data on their mobile/</td>
<td>2.9</td>
<td>3.0</td>
</tr>
<tr>
<td>portable device and using the data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>while in the field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using a cloud computing or SaaS</td>
<td>2.4</td>
<td>2.3</td>
</tr>
<tr>
<td>application</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Mean average ratings
Base: 320 respondents in August 2011 and 307 in March 2010
Data: InformationWeek Mobile Device Management and Security Survey of business technology professionals
Justify my wireless

Many organisations are finding that they are supporting more mobile phones than desktop phones. Yet, for the supporting network infrastructure, businesses are forced to determine objectives or directives to reduce capital and/or operational expenses. To make this decision, many organisations are looking at how their decisions on network investments are made today, to determine which investments are strategic versus those that could be deferred.

Several IT departments have already been asked to reduce network operating costs. As organisations search for ways to reduce opex or capex costs, many are finding it increasingly difficult to justify investments in their wireless network infrastructure. If your IT team has recently had to make an ad hoc or non-budgeted technology or support funding request related to mobile devices in your network environment, consider the problems caused by these requests.

Without a holistic view of the corporate network, IT can never be sure when it will need new wireless equipment or software upgrades, making it difficult to accurately budget and plan. Given that some of the rising costs of mobility, including physical deployment of tablets and devices, international roaming and dialling, day-to-day management and support of mobile users and their devices, are the result of uncontrolled expenses, you may have to take funding from other projects and, as a result, drop some of your value-add services.

Finally, the financial consequences of failing a network infrastructure compliance audit must be considered. Organisations must take into consideration the total cost – including potential penalties – of not passing a compliance audit. There are various compliance regulations and their penalties vary by regulation. But as an example, companies who fail to comply with the Payment Card Industry Data Security Standard (PCI-DSS) will lose their business relationship with VISA, Mastercard, etc. For organisations whose business is processing financial transactions, their livelihood is taken away. North American Electric Reliability Corporation Critical Infrastructure Protection institutes another compliance regulation around safeguarding North American power systems. Failure to comply with their standards will result in financial penalties for companies in the range of USD 1 million per day for egregious compliance violations.

Competition among mobile device companies for today’s mobile consumer is fierce, just as the competition is among businesses for attracting top talent in the recruiting process. Key to attracting this talent is mobile support. Many organisations today are concerned that their wireless network infrastructure is ill-equipped to offer the next generation of workers the ‘on-demand’ interactions they expect and that their network infrastructure will be unable to meet the future demands of the business.

Organisations need to plan for increased demands on the network and be able to increase its bandwidth as needed. Unfortunately, many organisations aren’t ready to support this next generation of workers and their preferred communications tools, creating a huge challenge from a business operations and IT support perspective. For instance, just 29% of the 551 business technology professionals who responded to the InformationWeek 2011 End-User Device Management Survey say they take a proactive approach to new consumer-centric technology, such as the Apple® iPad, in the enterprise. Additionally, 35% of these same respondents said they actively resist or outright ban new devices (see Figure 3 above).

An organisation’s inability to attract top talent to its workforce has a negative impact on their ability to compete – just think about the consequences of losing customers to your more agile and forward thinking competitors. Looking internally, consider the impact any gaps in your current enterprise mobility infrastructure will have on your ability to execute on future enhancements or projects.

When the organisation’s network cannot meet the demands of the business, the potential result is a lack of confidence in the IT department. This may ultimately impact business growth and strain the relationship between IT and the rest of the organisation.

Finally, if you don’t show a return on investment from network spending, less capital funding will be made available in the future.

Mitigate risk

As the trend to use personal mobile devices for business continues to permeate corporate networks, employees are demanding that IT services are delivered to their personal mobile devices. In light of this, organisations should follow IT governance models or implement internal network device configuration policies (e.g. ensure that IT has the ability to remotely wipe all mobile devices). For organisations that are governed by compliance and security-related legislation for data protection, there is plenty of pressure from the government as well (see Figure 4), requiring them to meet configuration standards across their network equipment and infrastructure.

As you introduce personal mobile devices to the corporate network, you must consider the challenges that you will face – from regulations and compliance to security. For instance, you may be concerned with the security of your wireless infrastructure as it relates to a security breach on your network. If there were a breach, you may or may not be equipped to restore your network. Many organisations are placing emphasis on improving their wireless network security, and are eliminating legacy mechanisms and implementing more advanced security for their infrastructure (see Figure 5).

There are plenty of actions to mitigate risk around users’ access to the wireless LAN.

- Securing client connectivity is critical. Many organisations require sufficient authentication mechanisms and effective encryption of data/communication as well as common security profiles across a wide array of wireless client devices. They’ll implement single sign-on and the 802.1x authentication standard for wired and wireless devices to enable simplified management, improved security and lower total cost of ownership. WPA2 + AES provide encryption of management frames. Fast Secure Roaming, LEAP and EAP-FAST can also secure client connectivity.

- Implementing secure guest access offers secure, controlled access to network services for non-employees and contractors. This will improve security while also lessening the workload of IT support staff if zero touch wireless guest services is implemented via an integrated stateful firewall for application level control of wireless traffic. This allows IT to control or block prohibited traffic patterns at a single point (e.g. peer to peer, instant messaging, file transfer protocol).

- Host intrusion prevention mechanisms address business challenges around standardisation on wireless client connection policies and protection from suspect content and potential hackers. Intrusion prevention systems provide enforcement of client connection policies around ad hoc wireless networks, SSID broadcasts and VPN connection at public hotspots. These systems can restrict wireless access when the device is connected to the wired network and prevent wireless clients from exploitation as a bridge into the wired network.

- Rogue detection capability protects network and information integrity from compromise by RF attacks and rogue access points or clients. Organisations can implement integrated 24/7 RF monitoring to identify, locate and contain unauthorised wireless activity. IT departments can also interface into original equipment manufacturer (OEM) management consoles for a single network management view and a more proactive threat defence to ensure regulatory compliance.

To determine your ability to protect the corporate network from potential breaches as a result of allowing personal mobile devices within the enterprise, take a look at your IT department. Do you have in-house expertise to identify, diagnose and remediate network problems in a timely manner? Many organisations don’t have IT staff to deal with risk issues, especially as we are witnessing an increased loss of qualified IT staff and greater difficulty replacing experienced IT personnel.

Now let’s discuss how to ensure that your WLAN is ready to meet new performance, integration, security and mobility demands at the lowest total cost of ownership.
Key challenges

Your choice of wireless LAN infrastructure is critical for both short- and long-term success. A smart access point (AP) architecture can handle the management function in an environment that does not need to scale to hundreds of users. But as business grows and the number of employees increases and security threats, such as rogue access points, ad hoc wireless networks and denial-of-service attacks, become even more critical to avoid, smart AP architectures may not scale to offer reliability, performance and safety. In that case, the use of a controller-based architecture will be necessary to handle the capacity and security requirements.

Another point to consider is that small branch offices may not have IT support on-premise, requiring the use of a WLAN controller to manage the branch office APs from headquarters.

When designing a high-density WLAN, take into account the performance implications of many tablets, smartphones and other Wi-Fi devices in a small area. Integration of multiple types of devices within a WLAN (802.11) technology environment must occur with ease. Today's newer mobile devices use 802.11n, and IT needs to ensure that they don't adversely affect the performance of clients using legacy Wi-Fi technology (802.11a/b/g), which is still around in many organisations.

To prevent performance degradation on the existing set of wireless devices and applications and ensure overall network performance, it's important to deploy 802.11n infrastructures from OEMs which incorporate beam-forming technology designed to improve downlink performance for all devices (802.11 a/g included) across one, two or three spatial streams. The beam-forming implementation ideally should not require client participation (sounding packet not needed) and creates transmit beam-forming implicitly between the AP and client to improve downlink traffic performance and range.

Security

Securing mobile devices is another challenge organisations face today. Obviously, there must be strong security measures in place, but the challenge lies in ensuring that mobile device users have convenient and seamless access to the corporate network while simultaneously protecting sensitive corporate data. As IT departments develop their approach to mobile device security, there are a growing number of compliance requirements that must be taken into account.

Securing personal mobile devices is no easy feat. Users expect seamless mobility when using their mobile device, regardless of whether it's for business or personal tasks, and IT must ensure that users can move across the corporate campus without interruption to or losing their wireless connection. In addition, IT must make sure that the network infrastructure is designed to improve the available battery life on mobile devices to improve the end-user experience, as well as productivity.
Infrastructure competency

In the first report of this series, ‘Ensuring Mobility Translates into Agility’, we discussed using an enterprise mobility framework as a guide when devising your enterprise mobility strategy. A key component of this framework is the network infrastructure. Organisations want to implement an infrastructure that achieves network singularity for users – or one seamless experience whether users are on campus Wi-Fi or public hotspots, home or branch office LANs, or even mobile broadband networks. We’ll explore this operational point of view further, for which we recommend a self-assessment, as it is a critical reflection point of enterprise mobility. We call this discipline infrastructure competency.

Its focus is on ensuring that wireless infrastructure (specifically the technical components used to deploy a wireless network) and mobile devices seamlessly support mobile and remote users. These networks are typically deployed in order to support business objectives such as improving productivity and increasing the responsiveness of a more flexible workforce. Within many organisations, employees are performing an increasing number of functions away from the physical desk or wired network connection. Because of this shift in working methods and patterns, it’s essential that the IT infrastructure continues to operationally support them with the same level of network performance as the wired network.

Levels of capability

In order to work out the levels of your infrastructure capability, there are a few possible levels of maturity, including basic, integrated and optimised. With each level of maturity, you can replace reactive mechanisms with more proactive approaches towards meeting an optimised infrastructure competency.

A basic capability in this competency would simply involve the provision for user connectivity supported by standalone access points with little or no management of connectivity, or performance-related metrics. This usually entails ad hoc wireless connectivity via standalone access points and limited connectivity for specific devices. For example, a business with basic capability might provide standalone access points set up in an office space so that a group of employees can work together, but security and user device support wouldn’t be robust and would usually be implemented in an ad hoc fashion.

As we move into an integrated capability, one should see the use of a controller to provide an authentication mechanism, as well as the ability to manage and control access points, based on standard WLAN technologies. Typically, there would also be device support using industry standards for security and communication. We should find next generation 802.11n wireless networks that intelligently manage connectivity in-line with capacity and performance. At this level of maturity, mobile devices are controlled according to business policy. We might also find that virtual WLANs are present to help segregate traffic by business function and thereby more efficiently handle the network load. This level of capability pertains to a much more intelligent, policy-based approach to connectivity that accounts for performance and capacity on the network. You might even have the controllers covering more access points over a larger area, such as a city area or college campus.

Optimised capability provides connectivity and support for mobile workers across the entire landscape, and is not limited to the wireless network. Mobility services such as voice, location or guest access are supported across wired and mobile service provider networks. Control, security and performance are incorporated seamlessly into all of these networks, while support and management is accomplished regardless of hardware specifics. For example, the support for operating systems and applications like Apple’s iOS or Google’s Android is the focus in the implementation of any mobility service. Device management is disaggregated from hardware specifics.

Examples

To help you ascertain where you are in terms of your capability within an infrastructure competency, below are some examples of mechanisms within an infrastructure competency:

- 802.11n wireless standard implemented to enable capability and reliability for voice, video, etc.
- Connectivity includes MESH topology to support communication in emergency situations, outdoor, or harsh environments
- Appropriate media gateways and routing platforms in place to support inter-connect with IP PBX and external networks
- Wireless coverage available across campus
- Wireless network supports multiple different user devices
- Windows Mobile and other mobile operating systems (Android, Apple, Blackberry, Symbian, etc.) devices supported
Questions you should ask:

- Do you have the 802.11n wireless standard implemented to enable capability for voice, video, etc.?
- Do you have the appropriate media gateways and routing platforms in place to support interconnection with IP PBX and external networks?
- Is wireless coverage available across the corporate campus?

The examples above can help you determine your desired future state. In your future state, consider which characteristics of your infrastructure you wish to have in order to meet business objectives around improving productivity of your workforce.

When you’re investigating the solutions you would like to implement to move to a higher maturity level in this area, consider:

- Do employees need a faster more reliable wireless network based on 802.11n?
- Would extended wireless coverage and performance across the company create more flexibility for your employees during their daily operation?

Conclusion

Organisations will need to support an increasing number of employee-owned personal mobile devices, such as smartphones and tablets. The ever-increasing number of these devices within the workplace will continue to add complexity as more manufacturers introduce their own devices to the market. These devices will be more bandwidth- and information-hungry than ever before, and IT departments will be presented with increasingly complex challenges, particularly in the areas of connectivity to the corporate network, back-end applications, device security and information security.

This need is becoming more pressing as tablet adoption continues and as the devices become commonplace in many organisations. In many cases, C-level adoption of tablets has accelerated the development of directives for IT departments to provide employees with the option to use tablets as a business tool. According to a recent Apple Inc., Quarterly Financial Report, 80% of the Fortune 100 is deploying the iPad in some capacity. Further, a 2011 data report by managed enterprise mobility vendor, Good Technology, found that iOS devices represented more than 65% of net new activations in the fourth quarter of 2010 within their customer base.

Reliability and performance of the network infrastructure are critical aspects when supporting a workforce on the move.

IT departments must prepare their wireless network infrastructures for tablets and other mobile devices, and provide mission-critical 802.11n wireless networks. Connectivity alone isn’t enough. Reliability and performance of the network infrastructure are critical aspects when supporting a workforce on the move. As more bandwidth-hungry applications and media content stream across the network to mobile devices, mechanisms that ensure scalable delivery of video applications to users must be in place. Most importantly, the infrastructure must support or enable users to securely connect to the corporate network via mobile devices.

It’s important to take a closer review of your infrastructure competency in addressing the aspects discussed above. Maybe you are at a basic level of ad hoc wireless connectivity via standalone access points and limited connectivity for specific devices. Perhaps you have controller-based WLAN wireless infrastructures in place and devices are supported based on common standards. The next step in your journey may be to implement a next-generation 802.11n wireless network that intelligently manages connectivity in line with capacity and performance, and where mobile devices are controlled according to business policy. The nirvana of seamless mobility services across wired, wireless and service provider networks, and device management disaggregated from hardware specifics may be well within your reach.

To be successful and realise the benefits of enterprise mobility, don’t forget that it’s critical to understand where you are today in terms of the capability of your infrastructure and where you need to be in the future to realise your goals. Now is the time to update and/or architect your IT infrastructure and associated policies to prepare for the inevitable continued influx of personal mobile devices into the workplace.

For more information, visit www.dimensiondata.com/enterprisemobility.