网络技术:强烈关注九大热门网络技术计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/584/2021_2022__E7_BD_91_E7_BB_9C_E6_8A_80_E6_c98_584481.htm 网络业是一个高度依赖技术创新与研发才能更好、更快地生存和发展的行业。但是任何创新的技术都不可能在一夜之间成熟并获得市场，许多技术的发展和市场普及需要数年甚至更长的时间，这也是为什么当我们展望新一年的热门技术时会发现，其中有很多技术是我们在上一年就一直在谈论甚至在使用的技术。2009年的热门技术展望也不会例外。 这里所列的2009年的9大热门网络技术，其实都是我们在2008年或者更早的时候就已经在使用的技术，但它们仍将是2009年的技术热点和市场热点。尤其在面对全球经济危机和企业支出日益缩减的情况时，真正热门的技术突出地体现了行业和企业对于它们的刚性需求，同时也明显地表明它们还负有帮助企业提高效率、降低成本，成功度过经济危机的潜在能力。正因为此，它们也才能担起2009年这一特殊而又关键年份的热门技术的名望。 1 802.11n：真正站稳脚跟 虽说WLAM早已有之，但是今年，因为有了802.11n，它才能最终立足。换句话说，从今年起，WLAN才会真正成为有线LAN的切实可行的替代者。 不必对WLAN以往的发展做很深的钻研，我们也能回忆起那些令人不快的发展历程：不成熟的WEP(有线等效安全)的实施、802.11b号称10Mbps但却很少能提供超过5Mbps的尴尬。802.11g号称50Mbps但却同样很少能提供超过20Mbps的窘境，以及围绕802.11n标准展开的旷日持久的争论等。的确，Wi-Fi技术一直以来的表现令人失望。一方面，我们开始逐渐地感

觉到，如果在家庭、咖啡馆、机场和旅馆中没有无线网络是多么的不方便。但是在办公场所，企业的员工，尤其是年轻的员工，对于无线网络的传输速率正逐渐失去耐心。而在《NetworkWorld》去年对208.11n的接入点和控制器进行的创新性的测试中，我们发现，802.11n接入点的速率可以达到令人印象深刻的250Mbps。此外，它在延时和数据抖动方面的可靠表现，表明它已能够支持像音频和视频之类的实时应用。我们所测试的系统拥有众多的企业级功能，例如PoE、动态射频控制、QoS、入侵防御和检测、WPA2和防火墙等。 企业在构建新的无线网络时，802.11n应当成为缺省选择。但是当企业已经部署有无线网络时，这种选择还是相当棘手的。如果企业已经有了802.11a/b/g，那么运行一个混合网络有可能会较大地减少带宽。在我们的测试中，混合网络的吞吐量只有全802.11n网络的24%。 但是不管你做出怎样的选择，802.11n已经做好了进入企业市场的准备。 2 统一通信：逐步升温 统一通信是这样一种技术，它似乎总是处在即将大规模爆发的边缘，但却不太可能真正爆发。原因或许就在于“ 统一通信 ”这个术语对于不同的人来说有着不同的含义。对电信经理来说，它意味着要用某个新创的开源企业甚至用基于微软的某个软件平台的IP-PBX去取代传统电信设备厂商久经考验的PBX。 而对桌面用户来说，它意味着将采用IP电话，并能享受到统一通信所带来的各种可提高生产效率的应用，比如音频和视频会议、即时通信以及语音邮件等等。 对于已习惯使用黑莓手机的移动员工来说，统一通信意味着可以将移动设备与办公室电话相连接从而实现所有的业务功能。他们可以将桌面电话转接到移动电话上，可以用移动电话拨打桌面

电话来阅读电子邮件和语音邮件，还可以将移动设备与桌面设备实行无缝同步。所有这些功能今天其实都已实现，很多大厂商，包括阿尔卡特-朗讯、Avaya、思科、IBM、微软、北电网络和西门子等都已能提供相应的产品。统一通信虽然不会让市场变得火热，但它在企业网中的普及速度却会很快。Nemertes研究公司最新的研究表明，在所调查的120家企业中，只有16%的企业没有采用统一通信。三分之一(36%)的企业已有了初步的部署规划.28%的企业已开始了有限的部署.另有19%的企业正在企业范围内全面部署统一通信。 那么，推动统一通信的发展动力是什么呢?去年4月，Gartner曾经调查过一些早期采用者，让他们列出部署统一通信的前三大好处，得到的答案是：员工的协作、员工的生产效率和分布式场所的通信能力。紧随其后的一个答案是TCO较低。 3 数据保护：从细节着手 在今天，当企业中的移动员工、远程办公、U盘、黑莓和社交网站越来越多的情况下，IT经理们已不可能再考虑如何控制这些设备的使用，而是需要关注如何保护数据的安全。一个很明确的保护重点就是笔记本(据估算，每年全美大约有5000台笔记本电脑丢失)的硬盘：它需要加密。 软件厂商，还有一些开源项目如TrueCrypt都能提供整盘的加密，微软在Vista里也提供了硬盘加密功能。除此之外，一些硬件厂商如富士通、日立和希捷等还提供基于硬件的加密功能。 另一个保护重点是电子邮件。现在有大量的电子邮件加密技术可供使用，但这些方法普遍存在一个共同的问题它们都要求加密邮件的接收者首先登录到一台安全的服务器上，然后必须输入一些确认信息方能访问解密的邮件。对于大多数人来说，这一过程是令人厌烦的。 保护电子邮件安全的

另外一种方法是数据损失防范，即DLP。DLP工具会扫描外发邮件，寻找其中是否含有诸如社会保险号、敏感的密码或其他可能导致数据泄露的信息。然后这些工具会对可疑的邮件进行标记，企业一般会要求将可疑邮件退回给发送者，或者退回给网络管理人员实施加密。 但是DLP产品要想顺利实施也并不容易。因为企业必须制定出详细的政策，决定哪类数据需要监测，一旦有电子邮件被标记该如何处理，个别人是否可以要求对一些特殊邮件或特殊类型的邮件实施加密等。举例来说，当CIO给CFO发送邮件时，如果因为其中含有一些机密信息而被做了标记、被退了回来或者被搁置了，那么CIO肯定会不高兴。还有一些可能存在问题的领域，从移动硬盘、U盘到智能手机比比皆是。不过，厂商们目前已可提供加密的U盘和带加密功能的商务手机。IT经理如今需要保护数据安全必须每一步都考虑周全。 4 绿色IT：环球同此凉热 实施绿色IT，企业是否负担得起?不实施绿色IT，企业能否承担因此带来的负面影响?这些问题都是企业的IT经理们必须面对的问题。 对于许多企业来说，走向绿色不过就是降低数据中心的能源消耗而已。到目前为止，节能的一些基本原则一般都能很好地被企业所理解比如整合服务器、安装冷热风通道、优化气流走向等。 这些改变可以节能，但是绿色IT决不能只停留在数据中心，企业更不能简单地把实施绿色IT的责任推卸给数据中心经理就算了事。IT部门可以而且应该承揽起大多数的绿色IT创新项目，而且这么做也不会花费多少钱。 首先，需要说服企业测量自己的碳足迹。这项工作是一个必要的起点。 一旦你对企业的碳足迹的大小有了感觉，然后就需要制定减排目标，比如说在特定时段内减排5%

或10%。这其中就包括了一些必须采取的行动： 适时关闭不用的服务器或台式机的电源 利用能效指标作为更换设备时购买网络设备、服务器和UPS的衡量标准。 采纳再循环和重复使用程序。 考虑可选的替代能源。 鼓励召开视频会议以减少热空气的流动。 敦促设备供应商必须制定绿色策略。 最后，不要被一些“ 粉饰绿色 ”的方式所欺骗。这些日子以来，每家厂商都声称自己是绿色的，但是企业必须验证他们的说法是否真实。 5 NAC：谋定后动 NAC(网络接入控制)在过去数年间一直很热。 关于NAC的标准之争让思科与微软处在了对立面，双方各有一套专门的术语和方法。再加上可信任计算组织(TCP)自己的一套架构，使得这一领域充满了变数。 还有一大批第三方厂商也在提供能够满足个别企业NAC需求的产品，他们是不会等待思科和微软的标准之争解决之后再动手的。 但是去年对于NAC来说是个转折点。标准之争似乎已经得到了解决。用户们很显然地决定等待微软发布其NAC产品，而让很多第三方厂商遭遇了冷落。 而且由于微软的NAC版本NAP(网络接入保护)可以随Vista和WindowsServer2008捆绑获得，所以对很多用户来说，决定跟随微软就成了一件不必费脑筋思考的事。NAP是一个简单而明确的选择，不必像RFP那样需要进行扩展研究、产品测试与评估等等工作。NAP在最近的产品评测中甚至已经证明了自己的实力。Forrester曾经做过一项研究分析，以便确定哪种NAC产品更能够解决现实世界的部署问题。结果微软的NAP名列第一，思科和Juniper位居其后。 今年对于用户的问题是，应该在何处部署NAC，以及需要打开多少NAC功能?很多用户现在使用NAC不过只是想控制访客的接入。其实这项技术可以做得

更多。在访客进入之前，它就可以扫描访客的设备，确定它们是否携带了病毒，检查它们的补丁是否已补齐，如果诸项安全条件不合格的设备则将被隔离。而在访客进入之后，它依然可以确保访客的设备是干净的，而且用户只能访问他们有权访问的网络部分。 这些重要的功能就是每个IT经理需要实施的部分。 