



工业园区网络解决方案

随着国家招商引资的步伐日益加大，各个地方的规划的工业园区、高新技术开发区等成为“筑巢引凤”的重要形式之一。目前国家优惠政策已经陆续落实，如何在基本持平的政策水平上获得更多厂商的青睐并入驻已经成为园区管理人员必须考虑的问题。

在政策等软环境已经就绪的情况下，提供完善的园区设施和配套服务必将是工业园区保持投资吸引力的建设重点。

网络的魅力——工业园区的新竞争优势

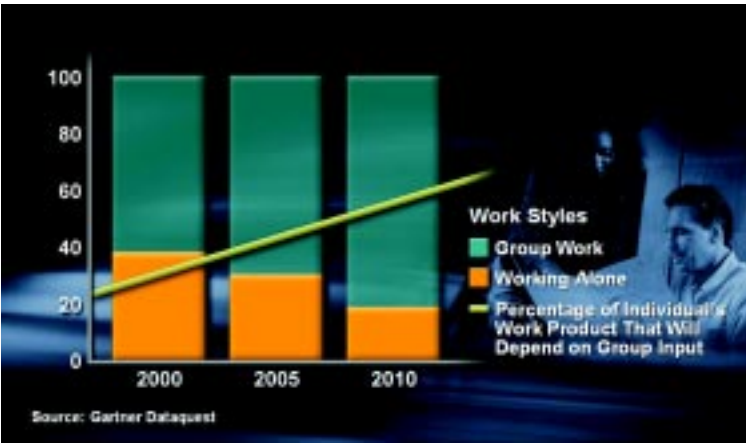
让员工效率提高 20%、工作场所的占地面积减少 40%、节省每个员工每天近 80 分钟时间……

提高效率 and 产能是厂商必须考虑的问题。随着办公场地费用的攀升，工作环境资源在企业商业活动的成本中占了最高的第二或第三位置，然而在正常的办公时间里，50%到70%的办公区间是空置的，无形中造成了巨大的浪费。为什么会出现这样的情况？

根据 Gartner Dataquest 的报告发现，我们的工作方式正在越来越趋向于团体的合作，在办公室里独立完成的工作越来越少。这就意味着：

- 一、工作时段我们必须完成的是协作性的工作。
- 二、在保证协作的同时，工作人员拥有更大的流动性，同时需要不同形式的沟通手段。

图 1
主要趋之一：在办公室里完成工作是由于不断增长的协作性需要



虽然协作的工作正在加大并占据了工作的主要部分，但是这并不意味着这两者有着鲜明的分割，报告显示，它们正在走向融合。传统的团体工作和独立工作往往与工作地点的选择密不可分。今天，通信技术已经让人挣脱了地域的限制，分散在世界各地的人员也可以组成团队，工作方式越来越灵活。

图 2
主要趋之二：向
灵活的协作性的
工作环境转变



面对日趋灵活的工作方式，作为基础设施的供应商——工业园区的管理者应该如何应变呢？

目前，国内大规模的制造型企业发展日趋平稳，新兴产业正全面向知识型经济靠拢，组织结构网络化，员工们掌握更多的知识和技术。提高员工效率，降低运营成本，面对国内处于涨势的人力成本和办公成本，网络成为实现一举多得的有效设施。

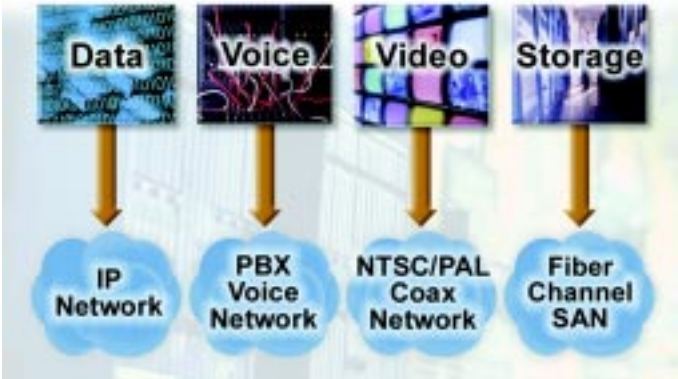
随着网络技术的不断发展，可靠稳定多元化的商业应用已经普及。网络已经成为企业的通信脉络。完善的园区才能吸引挑剔的厂商，如今园区网络化的趋势已是箭在弦上，蓄势待发。

新一代园区网的发展趋势

目前在企业中，往往多种网络并存，管理维护比较困难。基于 IP 网络的多网融合，为企业员工提供了灵活多便的沟通方式，大大提高企业运作效率。

在传统的大型企业中，通常有四种网络：1、IP 网络，用于传送数据；2、PBX 等电话网络用于传送语音；3、电视网络，主要用于传送来自生产线和安全监控摄像头的 PAL/NTSC 等格式的视频数据；4、存储网络，服务于 SAN 的光纤交换网络。

图 3
今天：独立分隔
的网络



多网并存无疑带来了更高的维护成本，对于入驻工业园区的厂商来讲，如果四套网络并存，则需要工业园提供四套完整的接口和相关设备，无论是从系统集成还是从园区管理人员的角度，显然是成本高昂的。

由于IP网络技术已经成熟，大中型企业已经具备了自有的企业网。经过改造后，单一的IP网络能够满足企业中的应用的多样性和实时性：

- 单一网络可以承载所有的信息流。
作为网络设备领域的领头羊，思科为广大的行业客户提供了最为全面的强大产品线，在关键领域内的能够满足实际应用中最为苛刻的需求。
- 降低复杂性：从厂商角度来讲，只需要维护一套IP网络。
从工业园区的管理者角度，集中铺设单一的网络也避免了各个企业各自铺设网络所带来的混乱。
- 节约成本。
由于各个企业都需要网络，由工业园区集中投入建设能够大大降低单位成本，单一的网络能够集中投入，提供更好的设施和服务从根本上保证高可用性。
- 利用IP网络在性能上的提高保证网络的实时性传播。
- 利用统一的网络访问具有战略意义的企业信息，提高生产率。
大中型企业大多拥有网络化的管理软件或企业Portal，通过统一的网络访问资源能够加强企业对于资源的掌控。对于园区的管理者，采用统一的IP网络，便于部署IP网络管理设备或软件，确保对厂商提供可控高效的网络服务。

图 4
聚合：语音，视频，
和存储都走向 IP



园区网络技术架构

由于工业园区处于一个基础设备提供商的角色，那么提供一个完善的、与入驻厂商无关、通用的IP网络平台是整个园区的基础。虽然厂商和园区可以同样汇聚到一个网络系统中，但是出于安全和管理，整个网络化地虚拟工业园必须分为两大类系统：园区管理系统和用户系统。

对于园区管理系统，需要实现

- 完善的多系统接入功能：
在工业园区的管理中涉及方方面面的单一功能自动化设备，如安检、访问控制、水电管理等。需要把这些单点的数据汇集起来
- 集成的楼宇自动化和安全管理
从各个终端采集到的各种类型的数据能够汇集并使得管理人员对于园区中的具体状况能够有直观的感知并管理

- 提供 IP 园区平台接口
对于接入网络的各个厂商，园区能够提供良好的接入设施和良好的园区网络服务让入驻的厂商能够像用电一样，一旦接入，网络无忧。

对于厂商的用户系统要实现：

- 完善的多系统接入功能
将客户的电话、传真、数据、视频等信号有效地汇集。
- 集成数据处理
从各个终端采集到的数据、语音和视频数据能够根据需求传输。
- 合理安全的网络接口
在享受园区网络服务的同时保证企业的网络安全。

图 5
工业园区网络：IT
及园区自动化系统的融合



工业园区基础网络方案

园区网络是面向众多不同类型的厂商，网络传输支持的不能仅仅限于数据。同时为了保证厂商的通信安全保证各个厂商间的通信相对独立，因此我们在园区网络设计上采用三层网络结构，即从逻辑上把网络分为三个层次：网络核心层、网络分发层和网络访问层。

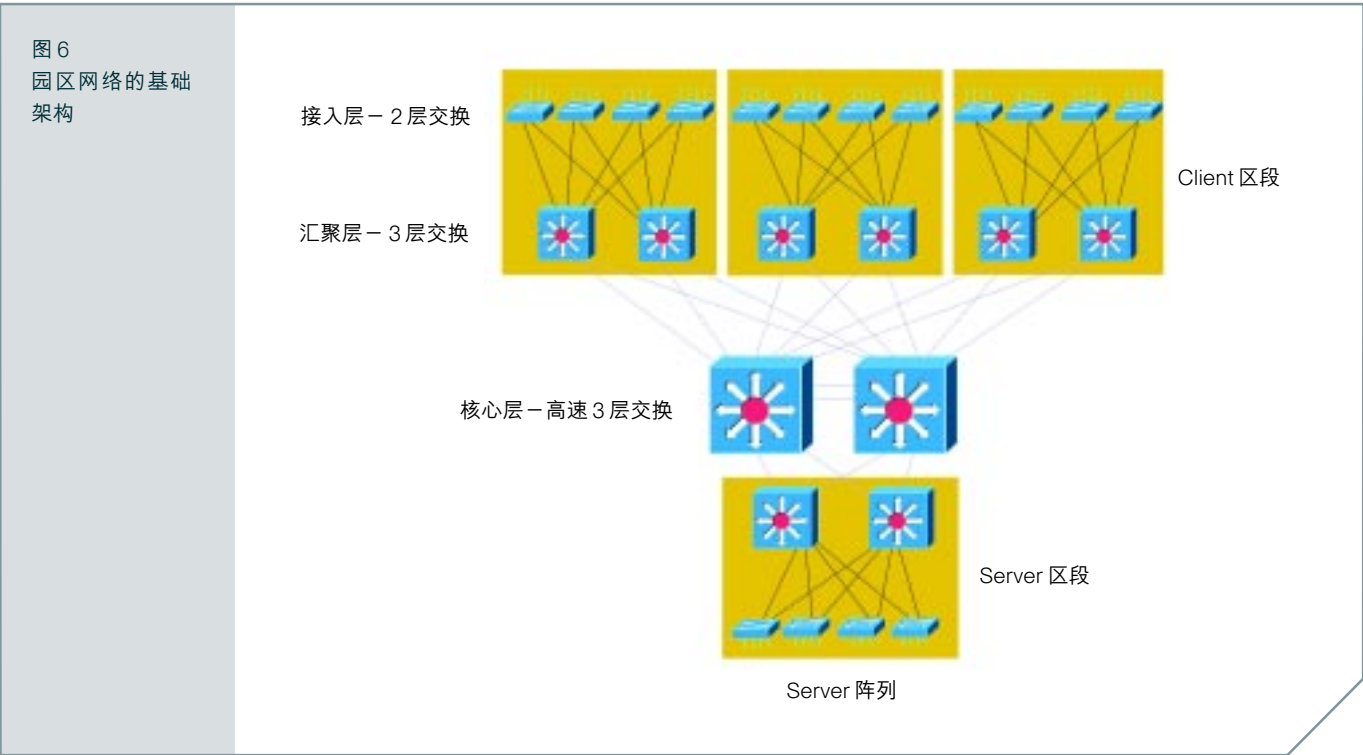
核心层是一个高速的交换主干，为应用层提供尽可能高的包交换速度，采用三层交换技术来保证核心层的带宽。分发层是访问层和核心层的分界点。这一层的目的在于定义核心层的边缘。在这一层处理用户数据包。其主要功能包括以下几个方面：部门和工作组的访问；广播和多点广播域的定义；vlan 路由；安全控制。访问层是最终用户访问网络的访问点，为用户提供网络访问能力其主要功能包括：为用户访问提供共享带宽；为用户访问提供交换 带宽；为用户提供地址分配，地址转换等地址服务功能。

多层次设计的原则：

- 集中与分散相结合，综合二层交换和三层交换的优势，降低复杂性
- 利用 IGP 使网络能够实现负载均衡、快速收敛、可伸缩性和可控性
- 在分发层和骨干网使用三层交技术
- 在子网使用二层交换及时，确保设备能够通过第三层实现安全、策略管理和 Qos

在实际应用中普通交换机由于工作在 OSI 7 层模型的第二层（即数据链路层），在划分子网和广播限制等方面提供的控制非常少，极容易造成网络拥塞，使数据包的丢失和延迟增加，服务质量无法保证。三层交换机则把网络通信中的二层交换技术和三层路由（或称三层转发）技术结合在一起，并通过 ASIC 技术达到线速交换，大幅度提高了设备数据的包转发能力，消除了转发瓶颈。同时通过 VLAN 划分、高效的组播控制、流策略的管理及访问控制等功能有效保证网络资源的充分利用，切实保证满足各类用户的应用需求。

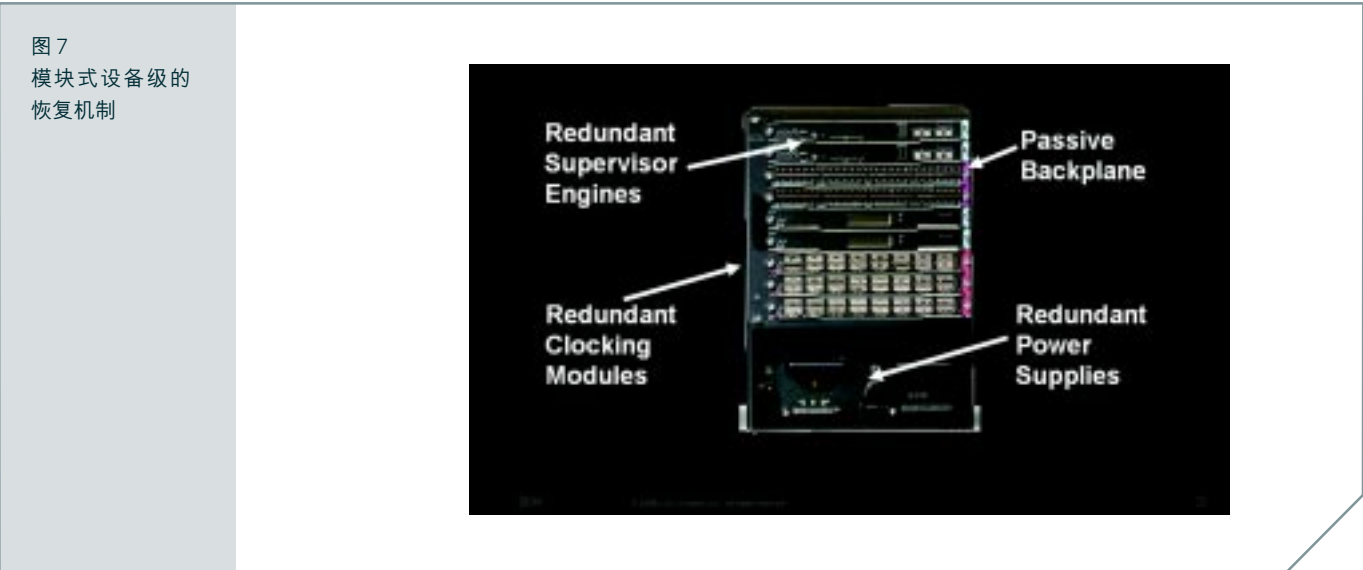
另一方面，随着网络规模的扩大，网络变的越来越复杂，网络在运行和管理方面所付出的代价。通常情况下，当园区用户转移到网络中另一个物理位置时，需要重新配置网络，甚至还有用户的工作站需要进行大量的管理工作。针对于此，三层交换机 VLAN 技术很好的解决了网络管理的问题。VLAN 的部署将通过减少网络中移动与变更所需要的资源，达到实现为用户节约资源的目的，同时 VLAN 能实现网络监督与管理的自动化，从而更有效的进行网络监控。远程管理，远程网络监控、故障报警等为网络管理员管理提供了有效的手段。



除了在网络设计方面尽可能保证园区网络的高可用性，在核心设备方面，思科为园区用户提供了完善的解决方案。

在核心层，思科提供了模块化的能够确保 365 × 24 不间断运行的可靠设备。普通的堆叠式设备随着堆叠数量的增多，复杂性相应提高，一旦出现问题，其中的故障设备就难以提供服务，而模块化的路由器提供多种恢复机制，除了支持热插拔，还提供数据包丢失保护，能够从网络故障中快速恢复。

此外，核心路由器还提供可实现快速的 1~3 秒状态故障切换冗余控制引擎、无源背板、IEEE 802.3ad 链路汇聚、IEEE 802.1s/w 和热备份路由器协议 / 虚拟路由器冗余协议（HSRP/VRRP）等多种手段来保证网络和设备弹性，确保园区能够向入驻厂商提供符合服务水平协议（SLA）的网络服务。



思科网络应用方案

在当今迅速变化的商业环境中，组织机构正面对日益激烈的竞争、利润的减少和业务模式的演变。过去关注的领域（如工作效率和客户满意度）此时比以往更重要，一些新的挑战因素如虚拟员工队伍的扩展、通信量的增长以及沟通方式的拓展和改变迫使企业寻求能够统一集成便捷的解决方案和管理办法。

为了帮助企业解决基于 IP 网络的解决方案和管理难题，思科在大力开发汇聚技术，将网络应用进一步整合，率先提供了完善的端对端应用，提供了包括 IP 通信、无线网络、网络安全、VPN 技术以及针对工业园区的网络管理等解决方案帮助客户降低总拥有成本，加强管理。

IP 通讯技术

IP 电话——收益最明显的 IT 投资

IP 电话是 VoIP（Voice over IP）技术的一种应用，作为数据网络发展的主要驱动力之一和一种革新性的话音业务，IP 电话一直倍受关注。目前已有很多厂商推出了自己的 IP 电话产品和解决方案，还有超过 20 家的组织正在参与 IP 电话技术标准的开发和推广。

Cisco 开放的 IP 电话结构提供了新型分组交换和开放计算技术带来的性能价格方面的益处，首次将呼叫控制技术引入开放环境，消除了对专用协议及封闭、嵌入和供应商专用软件的依赖。该结构基于标准的信息包基础设施层，由 Cisco 的 IP 和 ATM 骨干网、网关和接入解决方案组成。

图 8
Cisco整合的IP通信解决方案——业界最具发展潜力的,可管理的产品组合



除了在一般电话设备上提供服务，思科IP电话系统还能够为在统一的电话平台上的不同用户提供多种虚拟电话服务，如软电话（Soft Phone）、无线IP电话等等，以多种方式尽可能地为客户减少通讯开支。

实施了思科IP电话系统后，企业运营成本明显降低，效率提高，客户收到了非常显著的投资回报。如下图，根据Sage Research的一份调查报告显示思科IP电话后为园区企业和IT员工带来了非常明显的时间收益，提高了效率。

图 9
思科 IP 电话系统
投资回报报告



Source: Sage Research, January 2003

无线网络架构

部署无线网络——立刻提高 27% 的生产效率!

通过对 300 多家对 100 人以上规模的公司的调查发现:

- 每个月每个员工 45-60 个小时用来开会
- 每个员工大约只有 30%-40% 的时间会在自己的办公桌前
- 35% 的企业员工使用笔记本电脑
- 每个员工平均每天 3.64 个小时连入广域网

效率提高

不难发现,如果员工在非办公桌前 60%-70% 的时间内高效地使用网络,员工效率显然能够大大提高。根据详细的调查报告显示:部署了无线局域网后,平均每位员工每天能节省 80 分钟,工作平均效率提高 +27%,每位员工的开销仅仅提高 1%。

节约投入

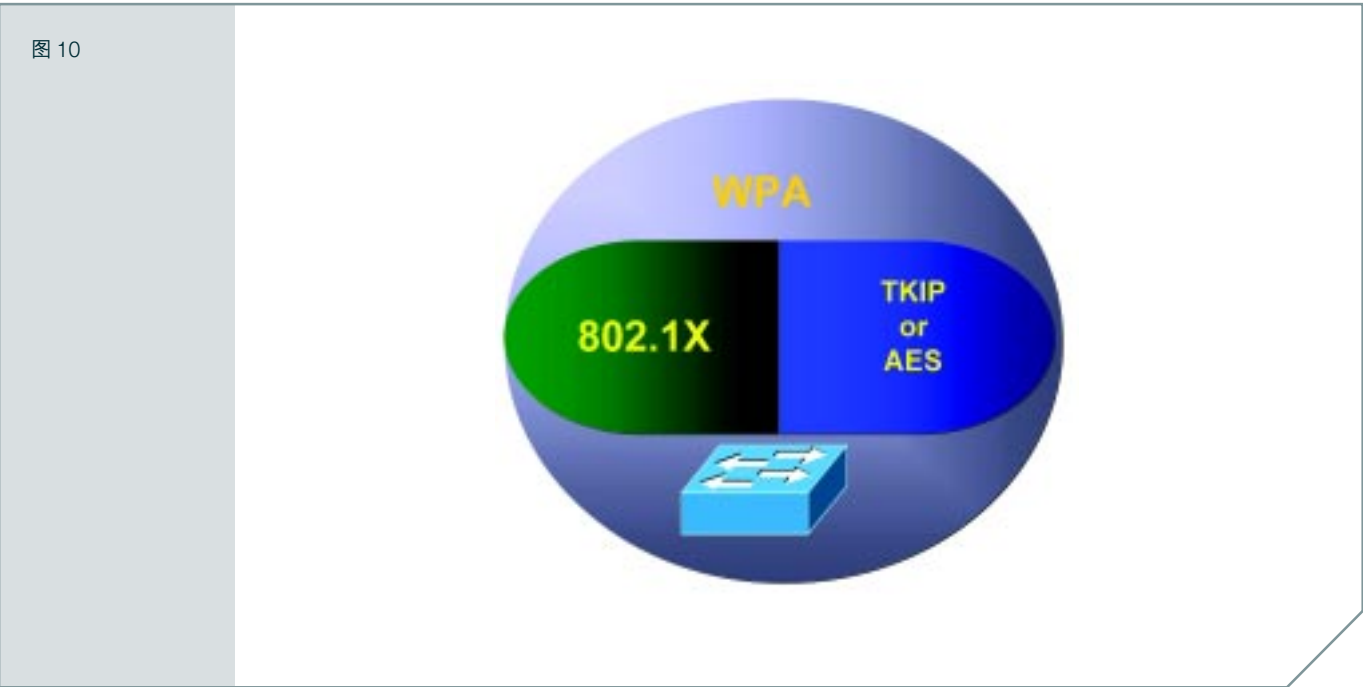
除了工作效率的提高,公司在网络基础设备上节省了相当的投入,免去了复杂的布线过程(尤其在很多不方便布线的场合)简化了日常的维护工作。尤其当办公地点变动或新增加办公室时,无线网络的灵活性和极低的实施成本能够帮助客户快速地开展业务。

可扩展性

除了在办公场所内部,楼宇之间和园区内均可部署思科无线网络。配合多种型号 IP 无线电话,思科为我们提供了富有创意的园区通信解决方案。

无线安全

无线网络在方便使用的同时,安全是一个不得不考虑的话题。思科无线网络在接入点集成了最先进的安全技术,采用 802.1x 提供的合法用户准入和 TKIP/AES (Temporal Key Integrity Protocol/Advanced Encryption Standard,临时密钥完整协议/高级加密标准),能够很准确地辨认接入者的身份,并配以对应的访问权限。





集成化安全及访问控制策略

建立了网络，必然会有人对它进行攻击，目前园区网络的安全主要受到两方面的威胁，一个是来自黑客的诸如 DoS 之类的攻击和黑客入侵，另外一个是有可能会被病毒感染。对于前者，最有效的解决安全的方法是设置内外网间防火墙（firewall）和入侵检测系统。而保证网络不受各种病毒的侵害，保证网络的正常运行，后者则应该配置网络防病毒软件。

网络整体安全设计

要想构建起来一个强大、安全的网络，一方面我们需要有强大的硬件平台作支撑，此外更重要的是我们要有严密合理的整体安全体系。

首先我们要严格定义和分类园区网的各种信息资源有哪些，其重要程度如何，需要访问这些资源有哪些用户，不同的用户所拥有那个等级的权限，同时将这些规则严格落实到最后防火墙 vlan 访问控制列表，arp 绑定等相应的规则的配置中去得以实现。对于从 Internet 过来的流量我们在 6509 上制定严密的限制性的安全策略采用特殊的许可与特殊的限制相结合，保证正常合法的流量的进入以及拒绝非法入侵。其次我们在本次园区网改造中所采用的网络设备，都支持 TACACS 的认证，应用这项技术可以使得对网络设备的访问控制可以集中设置、管理、授权。最后基于网络安全管理的重要性和防火墙保护范围的限制，这要求我们各个园区的管理部门进一步加强管理，制定相应的制度，加强防范，和防火墙一起配合，做到高度的安全。

这样我们可以很好的应用性能最为强大的防火墙设备结合防火墙的应用策略，网络设备的安全型配置，安全管理各个方面构筑起一道强大的安全屏障来有效地保障园区网的安全。

园区网络安全解决方案架构主要部分

- **身份识别。**身份识别是对网络用户、主机、应用、服务和资源的准确、积极的识别。实现它的标准技术包括验证协议，如 RADIUS 和 TACACS +、Kerberos 和一次性密码工具。数字证书、智能卡和目录服务等新技术正开始在身份识别解决方案中占越来越重要的作用。
- **外国安全 / 接入控制。**它提供了控制到关键网络应用、数据和服务的接入的方法，以便只有合法用户和信息可通过网络。带接入控制列表和/或状态防火墙、以及专用防火墙设施的路由器和交换机提供了这种控制。病毒搜索器和内容过滤器等补充性工具也有助于控制网络外围。
- **数据专用性。**当必须保护信息免遭窃听时，按需提供经过验证的保密通信的能力是十分重要的。有时，使用隧道技术，如 GRE 或 L2TP 来进行数据分离，可提供有效的数据私密性。然而，更高私密性要求常需要使用 IPSec 等数字加密技术和协议。在实施 VPN 时，这种添加的保护尤为重要。
- **安全监控。**为确保网络安全，重要的是定期测试和监控安全准备状态。网络易损点搜索器可主动发现弱点领域，IDS 可在发生安全事件时对其监控和响应。利用安全监控解决方案，机构可了解网络数据流和网络的安全状态。
- **策略管理。**随着网络规模和复杂度的增加，对集中策略管理工具的需求也随之提高。带可分析、截获、配置和监控安全策略状态的基于浏览器的用户界面的工具，提高了网络安全解决方案的可用性和有效性。

基于 802.1x 的用户接入认证

对于网络用户的动态接入认证，本方案选用基于 802.1x 国际标准的网络接入层用户认证协议，并在此基础上进一步利用思科公司的扩展功能对用户的 VLAN 划分，带宽资源分配和访问限制等进行动态设置。从而实现用户可以在园区网内的任何位置用自己的用户名和密码登陆网络，并获得相应的网络访问权限和工作组划分。

当用户的电脑通过网线连入接入交换机时，交换机会向用户的电脑发送认证请求。用户的用户名和密码等认证信息由交换机传送到网络中的思科认证服务器 ACS 进行用户认证，当用户的信息通过认证后，交换机才会开放用户所连接的网络设备端口，从而用户才可以获得对网络的访问许可。

思科基于 802.1x 的扩展功能 (IBNS)

思科支持 IEEE 802.1x 标准, 并且可以提供下述扩展功能以进一步增强基于 802.1x 的用户认证服务:

- 基于 802.1x 的用户 VLAN 动态划分:

Cisco IBNS 可以提供这种功能使基于用户的身份动态地将 VLAN 分配给相应端口。采用标准的 802.1 X 方案, 认证成功后的用户被置于预先配置好的 VLAN 中, 该 VLAN 已经分配到某个端口。这种新的特性使得管理员可以维护 RADIUS 内从用户名到 VLAN 的数据库。在成功地完成 802.1 X 鉴别之后, RADIUS 还可以将 VLAN 发送到用于特定用户的交换机, 交换机就可以为指定的 VLAN 配置附加端口。这样, 经过 802.1 X 认证的端口就可以将基于用户的身份指派到 VLAN 上。

- 带端口安全性的 802.1x

这种特性可以在 802.1x 端口上配置端口安全性。如果端口上只有一个介质接入控制 (MAC) 地址能够实现端口安全性, 那么只有该 MAC 地址才能够通过 RADIUS 服务器认证。所有其它 MAC 用户将被拒绝访问, 这样就能够消除其它用户连接到某个集线器上以绕过认证的安全性风险。在多种认证模式中采用带端口安全性功能的 802.1 X 时, 所有尝试通过交换机端口连接的主机都必须要求采用 802.1 X 进行认证。

- 802.1x 访客 VLAN

这种特性有助于让园区提供“访客”级网络接入, 如对于那些不支持 802.1x 的用户主机 (Windows98, WindowsMe 等)。在启用这种特性之后, 那些没有 802.1 X 兼容主机的网络的用户将被置于访客 VLAN 中, 他们可以获得 Internet 的访问权限或只可以访问园区网主页信息等。需要访问敏感资源的用户可以通过 VPN 连接来进行数据安全访问。

- 带 ACL 分配的 802.1 X

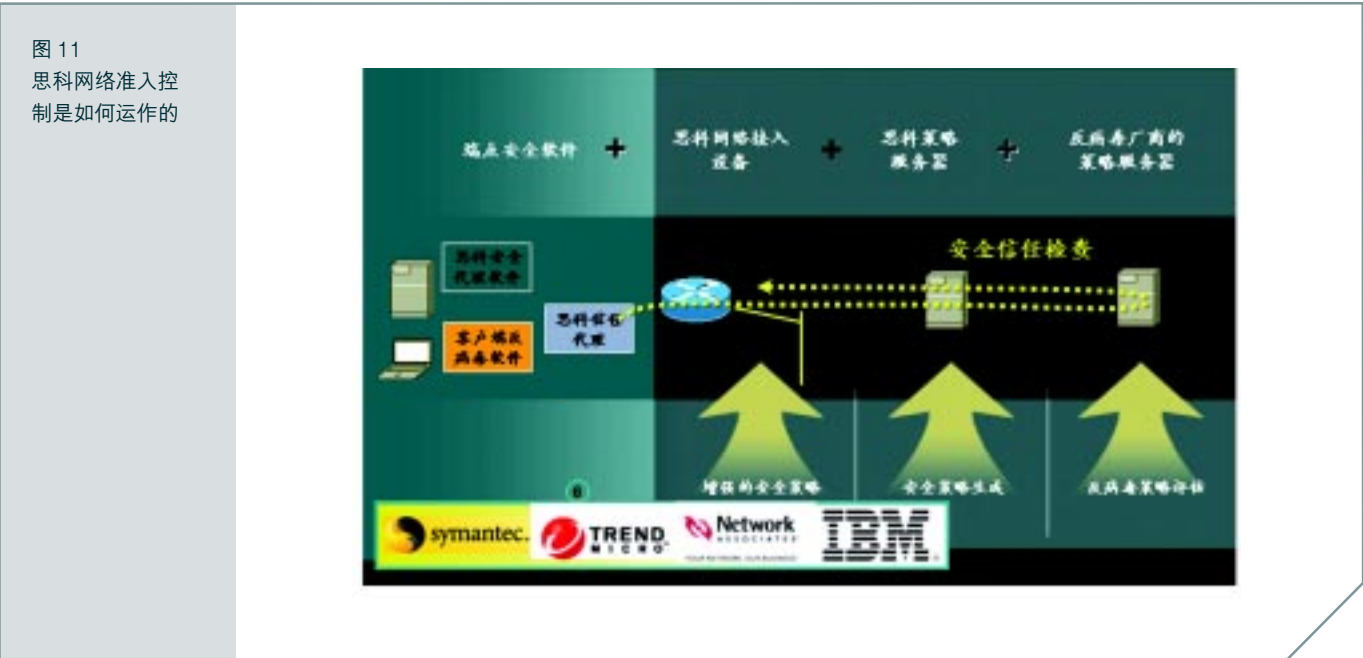
基于身份的访问控制列表 (ACL) 使网络可以根据用户的 802.1 X 认证结果, 动态地将访问控制策略分配到某个接口上。您可以使用这种特性来严格限制用户对网络中某些网段的访问, 限制对敏感服务器的访问, 甚至限制可能使用到的协议和应用。这样, 不需损害用户的移动性或者造成管理损耗, 就能够实现专门基于身份的安全性。

- 基于 802.1x 的机器认证

网络准入服务

思科网络准入控制 (NAC) 是一项由思科发起、多家厂商参加的计划, 其宗旨是防止病毒和蠕虫等新兴黑客技术对企业安全造成危害。借助 NAC, 客户可以只允许合法的、值得信任的端点设备 (例如 PC、服务器、PDA) 接入网络, 而不允许其它设备接入。在初始阶段, 当端点设备进入网络时, NAC 能够帮助思科路由器实施访问权限。此项决策可以根据端点设备的信息制定, 例如设备的当前防病毒状况以及操作系统补丁等。网络将按照客户制定的策略实行相应的准入控制决策: 允许、拒绝、隔离或限制。一开始, NAC 将支持运行 Microsoft® Windows NT、XP 和 2000 操作系统的端点设备。





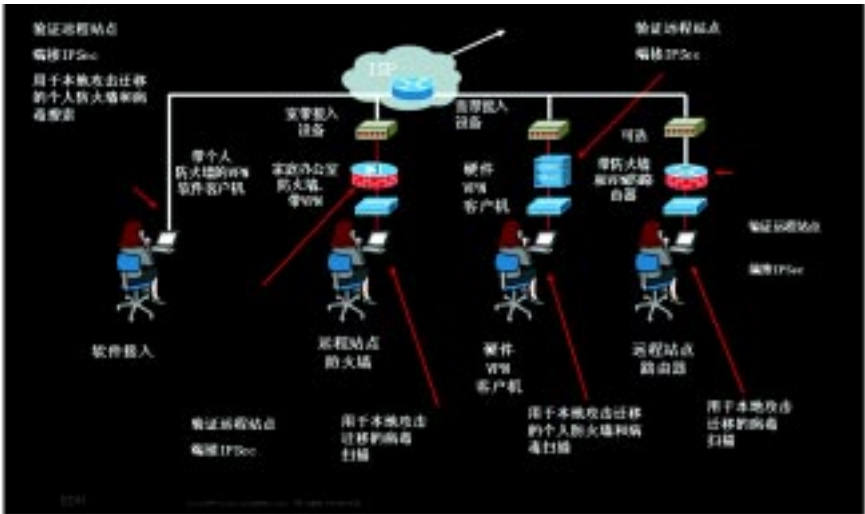
- 思科网络准入控制解决方案包括以下部件：
- **端点安全软件（AV，Cisco Security Agent）与 Cisco Trust Agent**——Cisco Trust Agent 从多个安全软件客户端收集安全状态信息，例如防病毒客户机软件，然后将这些信息传送到相连的思科网络，在那里实施准入控制决策。应用和操作系统状态信息，例如防病毒软件和操作系统补丁等级或委托书，都可以用于制定相应的网络接入决策。思科和 NAC 合作商将把 Cisco Trust Agent 与自己的安全软件客户端集成在一起。
 - **网络接入设备**——实施准入控制的网络设备包括路由器、交换机、无线接入点和安全设施。这些设备接受主机委托，然后将信息传送到策略服务器，在那里实施网络准入控制决策。网络将按照客户制定的策略实施相应的准入控制决策：允许、拒绝、隔离或限制。
 - **策略服务器**——策略服务器负责评估来自网络设备的端点安全信息，并决定应该使用哪种接入策略。Cisco Secure ACS 服务器是一种认证、授权和计费 RADIUS 服务器，它构成了策略服务器系统的基础。它可以与 NAC 合作商的应用服务器配合使用，提供更强的委托审核功能，例如防病毒策略服务器。
 - **管理服务器**——思科管理解决方案将提供相应的思科 NAC 组件，以及监控和报告操作工具。CiscoWorks VPN/ 安全管理解决方案（CiscoWorks VMS）和 CiscoWorks 安全信息管理器解决方案（CiscoWorks SIMS）形成了此功能的基础。思科的 NAC 合作商将为其端点安全软件提供管理解决方案。

虚拟专网应用

虚拟专用网 (VPN) 是部署于公共网络基础设施中的一种网络。它使用和专用网络相同的安全性、管理以及服务质量策略。使用 VPN 的优点包括：

- 降低成本
- 将连续性扩展到远程工作者、移动用户、远程办公室以及新用户（客户、供应商和合作伙伴）
- 能够对异地许可用户接入进行加密，确保数据安全传输。

图 12
Cisco 移动办公室
解决方案安全
灵活的远程接入



园区管理系统

面对如此庞大的园区网络，仅仅日常维护任务就相当艰巨。如何减轻我们的管理负担呢？在日常工作中，IT 管理员 70% 的工作都是在重复劳动，30% 的劳动才创造了新的价值。如何能把管理人员从烦冗的日常维护工作中解放出来？采用思科CiscoWorks2000网络管理软件就能迅速做到。

图 13
使用CiscoWorks
增强 IT 人员的
工作效率





CiscoWorks 为园区网提供了配置、管理、监控、故障检测与维修工具，同时还包括了用于管理局域网交换和路由环境的应用软件。

利用 Internet 的开放式标准及 Cisco 设备与操作系统的内在功能，园区网络管理解决方案使网络管理员能够有效地管理整个园区网。该决方案包括面向操作的多种工具，如故障管理、可扩展的拓扑检查、高级配置、第 2 层/第 3 层路径分析、语音支持路径追踪、流量监控、终端工作站跟踪工作流应用服务器管理以及设备故障维修等等。

网络管理包括两类：对设备和对应用的管理。建议采用 Cisco 公司的网络管理解决方案。Cisco 公司网络管理解决方案提供一整套完整的网络管理组件，其中包括对 Cisco 网络设备本身的管理以及对网络上传输的不同应用的管理等。

CiscoWorks 网络管理系统提供先进的网络发现技术，端口分配工具，复杂的网络连接分析，软件和配置管理工具，设备和网络诊断工具，和 RMON 远程网络流量监视，从而满足这些管理需求。

网络内容流的管理

网络内容流管理工具监视和管理服务器内容分配设备，如：Local Director，或其它 Cisco 具有负载均衡能力的设备。监视并维护关键应用在网络服务器中的流量分布。

网络流量管理

网络流量管理工具是综合性的网络流量监视，网络排错工具。它结合网络探索器，NAM 网络分析模块的使用，提供了 30 多种应用，用以监视网络的性能，网络的应用，网络排错，和网络历史数据统计，图形化显示和各种网络分析报告。

主要功能：

- 故障点孤立和排错
 - 内置报警提示网络性能的下降
 - 应用 TopNTalkers 发现网络错误
 - 在网络 7 层上全面分析 11 种网络协议
 - 收集统计网络 MIN、RMON 数据
- 强制策略管理
 - 通过为应用或用户制定带宽分配保障关键业务的网络资源
 - 通过实施基于应用的处理，支持按带宽应用的计费
 - 实时监视用户带宽的占用
- 网络性能调试和网络计划
 - 量化网络连接性能
 - 优化网络应用资源
 - 通过网络趋势预测并计划网络发展
 - 通过对网络的监视，提高全网络服务质量（QoS）

插入式模块：CiscoWorks2000 系列产品提供的开放式设计使 Cisco 可迅速增强产品功能以满足客户不断变化的需求。继推出 CiscoWorks2000 之后，Cisco 又将推出可提供新的或增强的网络管理功能的插入式模块。

思科管理服务

除了提供性能出众的设备和管理软件，思科还为用户提供了专业的管理和培训服务，全力协助园区为厂商提供满足服务水平协议（SLA）的网络。

网络服务租赁

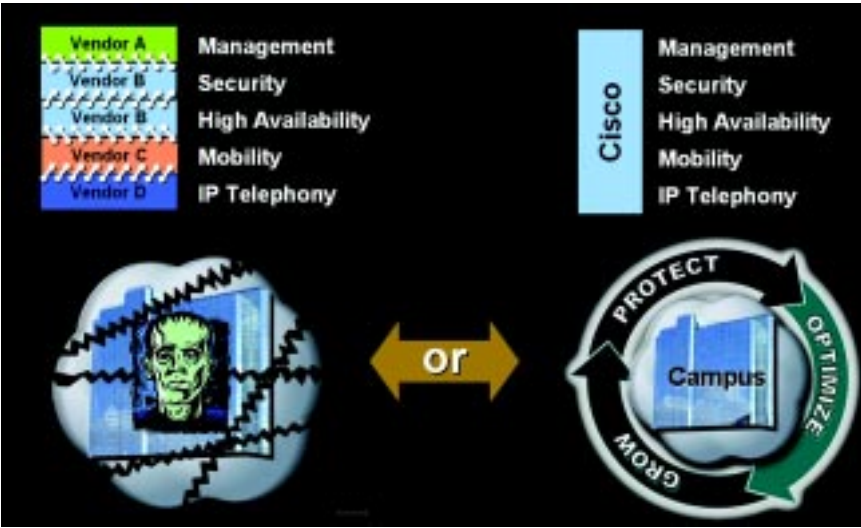
由于思科设备拥有良好的稳定性和安全性，为了避免网络设备性能闲置，园区管理者可以极低的附加成本将网络服务租赁给缺少设备和人力的中小厂商，进一步充分利用现有设备的同时，以高效的网络服务来吸引更多中小企业的进驻。思科网络设备为园区和厂商创造一个双赢的开始。

总结

“一体化”还是“四分五裂”？显然，思科拥有全面的网络解决方案和极具技术优势的全线产品和卓越的实施能力，能够将管理、安全、高可用、移动、IP 电话完美集成应用。企业也会因为全面的网络化而受益：更及时的风险管理、更有保障的安全性、更低的总拥有成本、更低的复杂性、更高的资源利用率——以及最终带来的更高的效率和利润。

思科提供的全面的企业网络架构能够进一步凸现商业价值。思科不仅仅带来了网络技术，还有更具价值的经验、最佳实践和完美执行力。

图 14
建设新一代的工业园区网络——建立全面的系统基础架构





思科系统（中国）网络技术有限公司

北京

北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19~21层
邮编: 100738
电话: (8610)85155000
传真: (8610)85181881

上海

上海市淮海中路222号
力宝广场32~33层
邮编: 200021
电话: (8621)33104777
传真: (8621)53966750

广州

广州市天河北路233号
中信广场43楼
邮编: 510620
电话: (8620)85193000
传真: (8620)38770077

成都

成都市顺城大街308号
冠城广场23层
邮编: 610017
电话: (8628)86961000
传真: (8628)86528999

如需了解思科公司的更多信息, 请浏览<http://www.cisco.com/cn>

思科系统（中国）网络技术有限公司版权所有。

2005 ©思科系统公司版权所有。该版权和/或其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS标识, Cisco Systems, Cisco Systems标识, Cisco Systems Cisco Press标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌, 名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。