"Wireless DeMilitarized Zone (WDMZ)" – Enterasys Networks' Best Practices Approach to an Interoperable WLAN Security Solution

Introduction

Wireless LANs (WLANs) continue to grow in popularity, particularly in enterprise networks. One attractive aspect of WLANs is their ease of deployment. For instance, wireless networks can be deployed without the installation of massive amounts of cabling to the desktop. In addition, mobile, ubiquitous access throughout the global enterprise yields a more productive and efficient workforce, since employees can access resources without being tethered to a wired network connection.

WLANs have also spawned a paradigm shift in how network architects approach the issue of security. Typically in the past, physical security controls were considered sufficient to ensure that no unauthorized person could gain access to the corporate network. However, wireless networks expand Layer 1 access to areas such as parking lots and adjacent office space; thus, physical controls are no longer sufficient to maintain the security of enterprise networks.

The IEEE 802.11 committee had this issue in mind when it incorporated an encryption mechanism known as Wired Equivalent Privacy (WEP) in the 802.11b wireless communications standard. Since its ratification, WEP has become standard on nearly all 11Mbs wireless products based on the standard and is a minimum qualification for certification under the Wireless Ethernet Compatibility Alliance's (WECA) Wi-Fi™ interoperability standard. In addition to utilizing WEP, as a further security feature, many vendors have offered a 128-bit version of the RC4 encryption that forms the basis of WEP.

WEP has generally been viewed by enterprises as a mechanism to lessen the risk of the interception of data by unauthorized entities, to provide some access control to prevent unauthorized use of the network, and to offer a measure of data integrity to ensure that messages were not tampered with while in transit. However, the publication of a white paper entitled "Intercepting Mobile Communications – The Insecurity of 802.11" written by Nikita Borisov et al. from UC Berkeley, accompanied by an ensuing tidal wave of negative press coverage, began to dissolve confidence in the WEP approach.

Enterasys Networks acknowledged the vulnerabilities of WEP in a position paper entitled "Enterasys Position Regarding WEP" (published in February 2001) and advocated the deployment of additional security mechanisms within the enterprise for the transmission of sensitive data using WLANs. Interestingly, the Gartner Group echoed this position in a research note entitled "Deploying Safe Wireless LANs", published in July 2001, which advocated the deployment of virtual private network (VPN) technology with wireless installations in enterprises where multi-vendor interoperability is a requirement.

The keen focus on security further intensified in August 2001 with the publication of yet another white paper after a new attack devised by three well-known cryptographers and successfully repeated by a team of AT&T Labs researchers was presented at a conference in Toronto. This new approach and ensuing documentation demonstrated that the time and cost estimated to complete a WLAN hack as described in the UC Berkeley paper had been vastly overstated. In other words, this white paper pointed out that breaching WLAN security is potentially an even simpler task than had been previously noted.

Since the publication of these papers, effectively the state of WLAN security has not changed. WEP remains an adequate mechanism for prevention of casual eavesdropping and low-level authentication. However, the Wall Street Journal on April 27, 2001, described a test in which two hackers with a laptop drove through Silicon Valley and were able to access multiple corporate networks. The unfortunate reality is that, even today, most enterprises do not enable WEP, traditional authentication mechanisms such as Radius, or even an SSID network name. In another research note, entitled "Pirate Radio: Wireless Insecurity Through Users," Gartner recommends the use of these security tools as part of a minimum standard in deploying all WLANs. In addition, Gartner recommends implementing MAC address tracking to control network security and the use of network-based intrusion detection to identify unauthorized access or attack.

Most importantly, enterprises must develop and publish standards and policies for the deployment and use of WLANs. The development of these policies should require an honest risk-assessment and a comprehensive security health-check of the entire network. Enterasys and its partners can assist in this process. Once the risks and vulnerabilities are identified, Enterasys can craft solutions using an array of technologies from its Secure Harbor portfolio, in conjunction with third-party offerings.

Some vendors have proposed the use of proprietary per-user or per-session encryption capabilities as an answer to recent wireless security concerns. While these solutions are arguably more robust than WEP alone, they may strengthen authentication and encryption capabilities while sacrificing performance and roaming capabilities. Furthermore, most of these solutions require a proprietary management system and protocol (and, in some cases, additional network hardware) for implementation. None of these solutions serve to integrate these new security measures for the benefit of the entire network architecture. In addition, all of these approaches have sacrificed vendor interoperability. For most enterprise-class networks, these trade-offs are simply not viable options and do not support the value proposition behind the initial choice to deploy wireless networking.

The IEEE 802.11i Task Force is currently working to address the vulnerabilities in 802.11 WEP. Enterasys is participating in the process and will implement the new standard, once ratified, in its RoamAbout R2 Wireless Access Platform.

Because every enterprise architecture is unique, every risk assessment is unique, and every asset inventory is unique, therefore Enterasys Networks proposes a "Best

Practices" approach to wireless security that leverages flexibility and value for every enterprise, regardless of the vendor mix. When an enterprise's risk profile makes it vulnerable to determined attacks, Enterasys recommends following the best practices to secure their wireless network.

Requirements of Wireless LANs (WLAN)

To understand the environment and the objectives of these practices, review the objectives of a wireless network environment. In doing so, remember that a wireless network uses a public medium (the airwaves) for its transmission. Without any protection, it is like being directly connected to the Internet, with the added twist that an intruder does not require any physical connection to eavesdrop.

Connecting this public medium to your enterprise network requires addressing the following functions and issues:

- Compartmentalization
- Secure Intranet Access
- Data Confidentiality
- Access Controls
- Bandwidth Management
- Intrusion Detection
- User Roaming
- Multi-site Consistency
- Wireless Card Interoperability
- Access Point Management
- Access Point Security

The optimal method to address these requirements is with the use of a Wireless DeMilitarized Zone (WDMZ). The requirements as well as how they are implemented in the WDMZ framework are discussed in detail in the following sections:

Compartmentalization

In order to apply the best practices to all wireless devices, wireless LANs must be segregated from the rest of the enterprise network. Wireless access users may not be trusted to the same degree as wired LAN-attached devices and thus need specific management. This segregation allows appropriate policies to be applied to these wireless devices.

The segregation of a wireless LAN can be accomplished via a separate physical network or a VLAN that contains all of the wireless access points and no other enterprise resources. This compartment is called a Wireless DMZ (WDMZ). Just as with Internet access, this WDMZ is established as an intermediate network that is mostly secured, but not fully trusted. A DHCP server dedicated to this network will assign wireless users their addresses when connecting to the WDMZ.

Secure Intranet Access

Once the wireless devices have been segregated, controlled access to the enterprise intranet must be provided. Since a wireless network is not bound by any doors or walls to prevent unauthorized connections, devices connected to the wireless network must be authenticated and authorized before trusting them on the enterprise network. Wireless users and devices must be known to the enterprise and the enterprise must decide and enforce the level of access to be granted.

Wireless users should be authenticated and authorization received every time they connect to the WDMZ. This authentication should re-utilize the mechanisms already in place to perform these functions. Typically these are based on RADIUS or a token-based method, such as SecurID. With this in mind, the IEEE has standardized 802.1x as an extensible protocol for LAN authentication. Windows XP will support this protocol natively and this is an ideal method for user authentication and authorization.

Some legacy systems will not have support for 802.1x. In these cases, or in order to achieve data confidentiality, a VPN should perform authentication tasks.

Data Confidentiality

Current wireless encryption technology and standards for data confidentiality are in their first generation. The predominant standard is Wired Equivalent Privacy (WEP). Like other first generation encryption standards for other means of access, WEP provides basic security, but weaknesses are being uncovered which a determined attacker could exploit.

The disclosure of these vulnerabilities has led some manufacturers to develop “band-aid” mechanisms in attempts to correct the flaws in WEP. However, these typically address only published attacks and don’t address the fundamental designs of the protocol. Security protocols are difficult to evaluate and need adequate time to develop and submit to stringent peer review. The IEEE is following that path to develop a second-generation solution. A solution is urgently needed, but rushing this process would not yield a highly secure solution.

In order to bridge the gap until second-generation security can be developed and standardized, analysts and industry experts recommend utilizing the proven security of IPsec VPNs to secure data on wireless LANs. Secure VPNs are already in their second-generation, having made the same errors exhibited by WEP in their own first-generation. Their objective is to permit secure communication over an unsecured network. That unsecured network has typically been the public Internet (with respect to VPN proliferation), but the public airwaves are simply another unsecured medium to which VPNs add value.

Access Controls

Best security practices envelop multiple layers and technologies to create a secure environment. Knowing that wireless access is less controlled than physical connection, best practices will limit certain types of access from wireless devices. For example, modification of user profiles or network reconfiguration may be restricted from access via the WDMZ. In this example, an attacker that achieved brief access would be prevented from opening a permanent hole.

The security staff should review access requirements for the WDMZ and block any protocol or subnet access that doesn't have strong productivity motivation. By utilizing the gateway from the WDMZ this access can be applied as access is granted onto the intranet. This could be in the VPN gateway or the campus router behind the gateway, depending on the sophistication of the rules.

Bandwidth Management

Wireless bandwidth is and will continue to be scarce when compared with wire-line technologies. Enterprise policy, applications, and wireless access point density interact to determine how the wireless network will perform. For example, a wireless network with sparsely placed access points and little overlap may suit the needs for of an organization that uses wireless LANs for conference room email access. However, this same network could crumble if used for shared server infrastructure and network intensive design tools for office space.

Wireless networks can be designed with a broad range of available bandwidth. The best practices use the WDMZ gateway, discussed in prior sections, to enforce data traffic rules insuring the wireless LAN is used for its intended purposes.

Intrusion Detection

Wireless LANs make attractive attack points for intruders. The discovery of attacks can point to a need for greater perimeter observation and could be the trigger to increase visual and electronic surveillance. A wireless attack is far more targeted than an internet probe. In the wireless LAN case, the intruder is in generally close physical proximity (usually <100 meters from an access point) and has most likely targeted your specific enterprise. If the wireless attack fails, the intruder may proceed to other offensive methods.

The WDMZ is particularly effective in discovering these attacks. The best WDMZs will include an intrusion detection system to capture these activities and alert the proper staff.

User Roaming

One of the greatest benefits of a wireless LAN is mobility around the office. Workers can take their laptops throughout the enterprise space, all the while seamlessly connected, without requiring re-authentication or session loss. As the WDMZ and security overlays are put in place, these attributes should not be lost.

Some vendor solutions increase security to a single access point, but lose the ability to roam among access points. These limitations may meet user resistance, potentially resulting in pressure to lower and lessen security. The best security solution needs to provide for roaming. By using a VPN connection, the security is from the workstation to the WDMZ's network gateway. The access point in use is transparent and roaming is seamless.

Multi-site Consistency

In addition to the productivity benefits of wireless LANs on the enterprise campus, use of the technology as a single method of access in other enterprise sites, hotels, airports, and the home broadens the overall productivity of enterprise wireless access.
WDMZs must enable multiple-site access with minimum reconfiguration, and without reducing overall security. For large remote sites, this means a parallel WDMZ with the same configuration as the central site. For smaller sites, routing WDMZ traffic to a central WDMZ for network access controls can minimize the costs of the WDMZ infrastructure.

Wireless Card Interoperability

WI-FI™ interoperability, having been proven and certified by the wireless LAN industry, has been widely adopted and has contributed to the explosion in wireless LAN utilization. Interoperable technology insures that a card used in one facility will work in another facility, at home, in the airport, at a convention, or even in the local Starbucks. Interoperability grants the user freedom to use whatever access card he or she has available. Now that PCs are now shipping with wireless functionality as an integrated component, interoperability is critical for seamless and productive wireless LAN deployments.

The WDMZ approach preserves this capability and strengthens it. Since the security layer is structured around the wireless connection, any WI-FI™ network card can be used without compromising security. On the other hand, WDMZs will protect the enterprise network from unauthorized access by other interoperable cards.

Access Point Management

Not to be forgotten in this discussion is access point management. The best WDMZ will have high-powered access point management to monitor access point performance, evaluate loads, and manage configurations. These access point managers must be securely configured against attack. Ideally, these managers would only be "ON" in the network during actual management operations.

Access Point Security - First line of Defense on the DMZ

The security mechanisms offered in 802.11b and the subsequent implementations of 128-bit WEP can and should serve as the first defense barrier. These include implementation of an SSID or Secure Network Name. Some vendors offer a "secure access" mode that will enforce use of a unique SSID among clients and prevent "beaconing" of that SSID name from the access point. Radius-based authentication of user MAC addresses or static MAC Access Control Lists should be implemented whenever possible. 128-bit WEP is recommended, as well as regular rotation of encryption keys. Some vendors offer utilities to automate the process of changing keys.

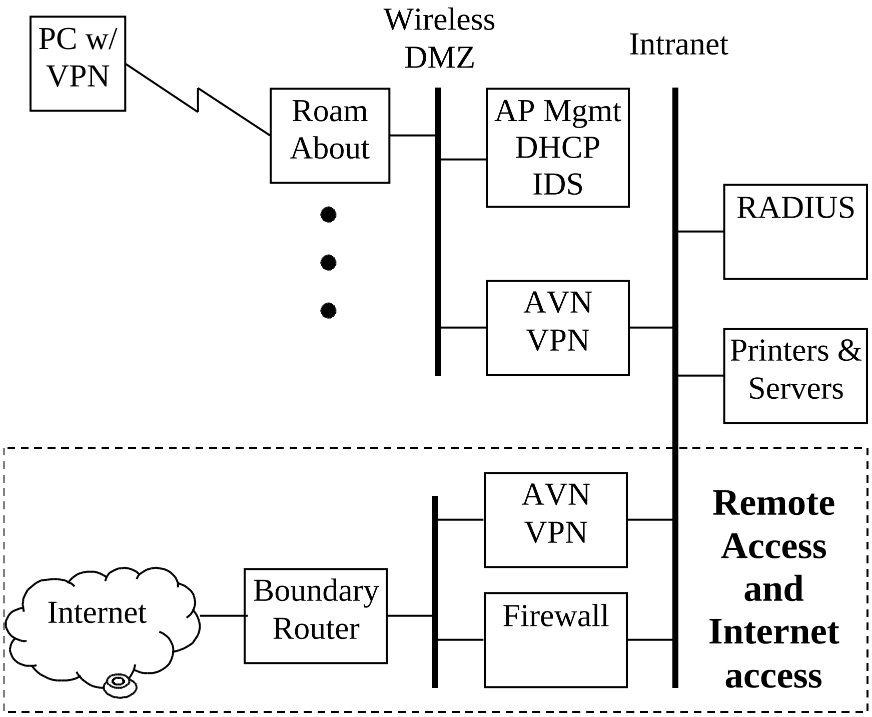
Wireless DMZ Configurations

In order to apply the best practices to understandable configurations, the following sections illustrate how the WDMZ would be configured in several situations. These illustrations are intended to serve as flexible and scalable design models.

Basic Data Center Configuration

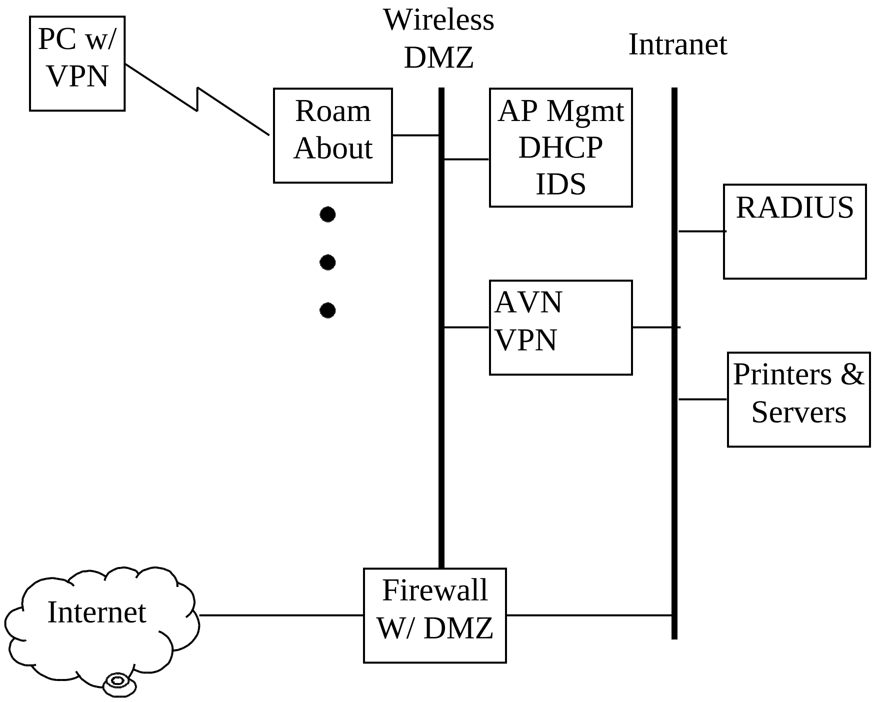
The configuration below represents a data center that is using a VPN for remote user access as well as for WDMZ protection. In this example, separate VPN gateways are used for the highest level of segmentation and security. Separate Internet and Wireless DMZ's eliminate the possibility of configuration errors that could permit Internet attacks against wireless PCs.

Notice that the WDMZ has its own resources for DHCP address assignment and intrusion detection as described above. All access to the enterprise intranet is via the VPN gateway. This gateway or a campus router would perform filtering and bandwidth management.



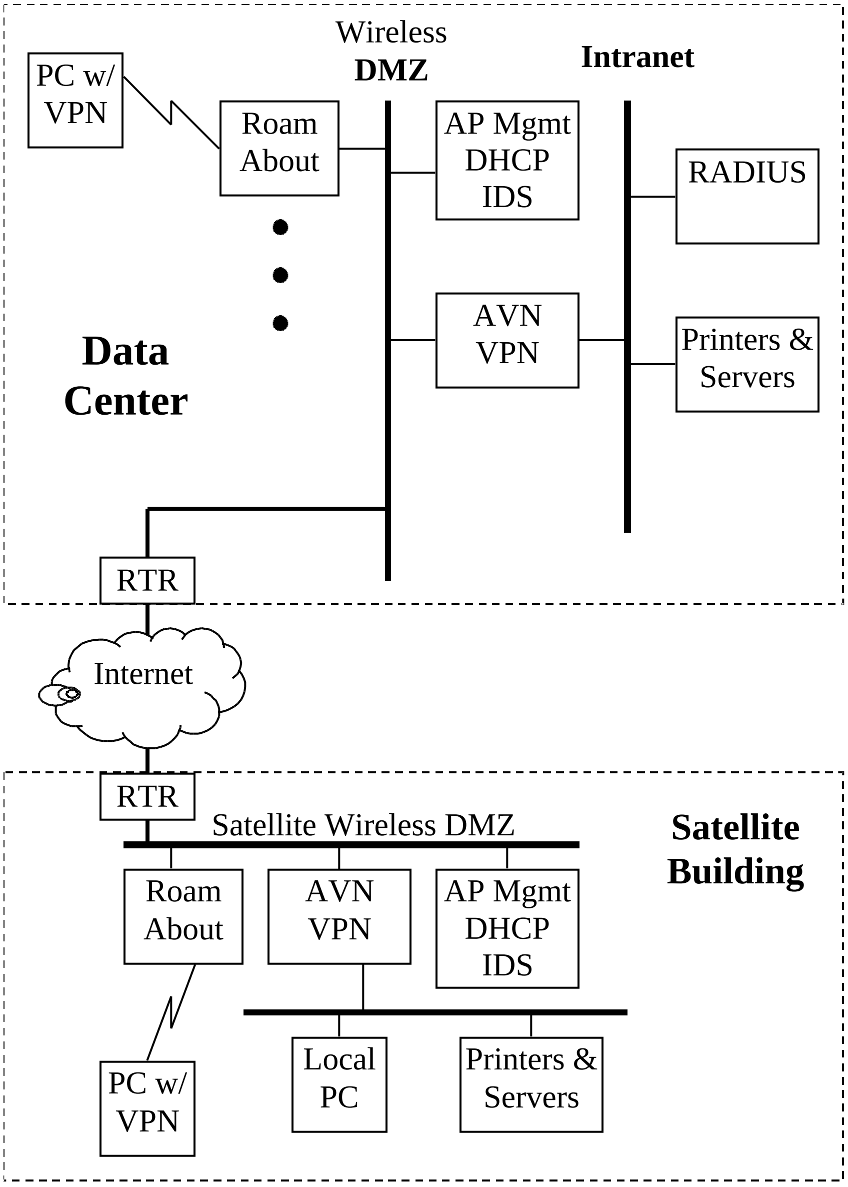
Firewall with DMZ Data Center Option

This example shows an option for connecting the WDMZ onto a firewall DMZ port. This solution can contain costs in some networks by permitting a common VPN gateway to serve remote access and wireless needs. This solution is less secure than the dedicated approach, since the complexity of firewall rules could accidentally permit attacks on WDMZ users. However, cost constraints may necessitate this approach.



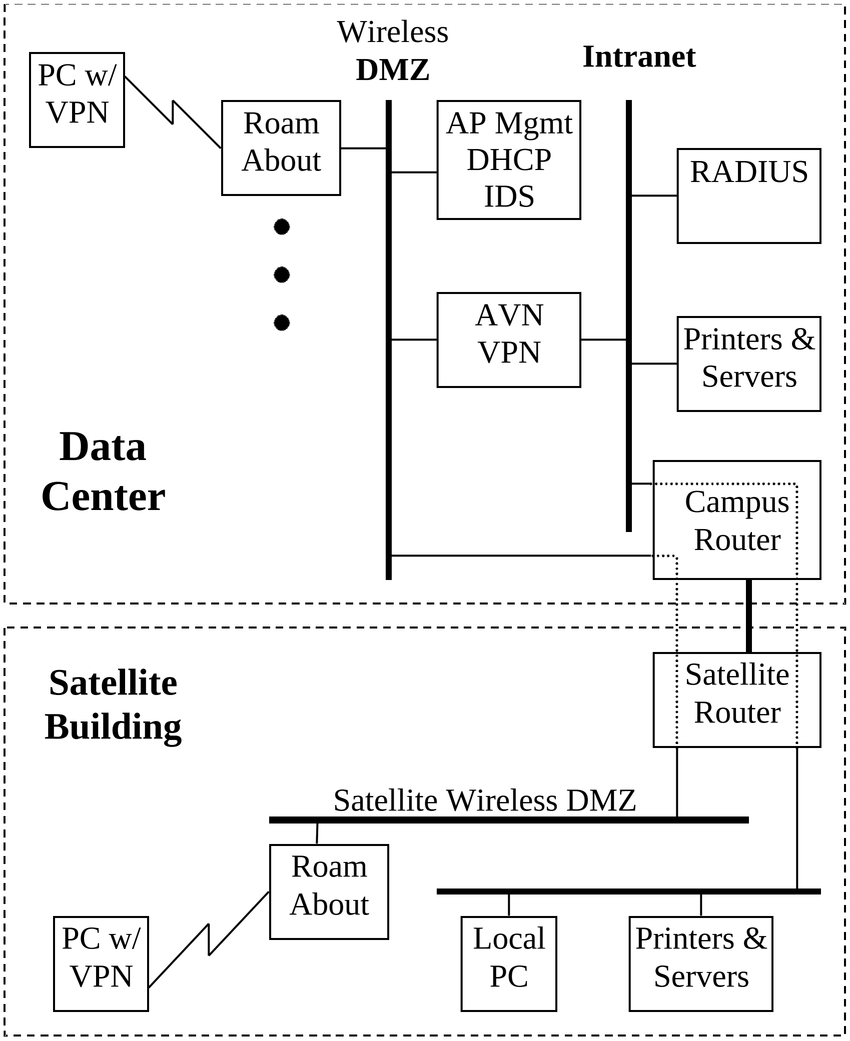
Satellite Office Configuration

Remote offices may not have enough users or wireless bandwidth traffic to justify their own WDMZ gateway. These cases present an opportunity to combine the approaches described in the prior section, by using a VPN gateway to protect the WDMZ and to establish site-to-site connections. In the diagram below, the VPN gateways are providing the connections between the two sites, and they are also used to connect the WDMZ into the enterprise network.



Alternate Satellite Office Configuration

Here is another case in which remote offices may not have enough users or wireless bandwidth traffic to justify their own WDMZ gateway. Frequently the bulk of the traffic in these sites is destined for the data center mail or application servers. In these cases, little network overhead is needed to route all of the WDMZ traffic to the data center's WDMZ for access control to the enterprise intranet. The satellite and campus routers would be configured to restrict WDMZ traffic to only flow to the other WDMZ.


PC w/ VPN
Wireless
DMZ
Intranet
Roam About
AP Mgmt
DHCP
IDS
RADIUS
AVN
VPN
Printers & Servers
Data Center
Campus Router
Satellite Building
Satellite Router
Satellite Wireless DMZ
Roam About
PC w/ VPN
Local PC
Printers & Servers