

Allworx 10x Networking White Paper



-PAGE INTENTIONALLY LEFT BLANK-

Table of Contents

1	Introduction	1
2	The WAN Interface and your Internet Service Provider (ISP).....	2
3	IP Addresses, Netmasks, Gateways.....	3
4	Allworx Networking Security - Firewalls and NAT	4
4.1	Firewall.....	4
4.2	Network Address Translation (NAT)	4
4.3	Mode Summary.....	5
5	Dynamic Host Configuration Protocol (DHCP)	6
6	Domain Name Server (DNS) and Domain Names.....	8
6.1	Settings Summary.....	8
7	Mail Configuration and Unified Messaging	10
8	Allworx as the Primary Mailbox.....	12
8.1	Inbound via SMTP	12
8.2	Inbound via POP3.....	12
8.3	Mailbox Access	13
9	Allworx as a Secondary Mailbox.....	14
9.1	Pull Model: Unified at the Client.....	14
9.2	Push Model: Replicated by Allworx.....	14
10	Advanced Topic: Using Allworx to host your DNS Domain.....	15
11	Advanced Topic: IP Telephony and Quality of Service Issues	21
11.1	WAN VoIP	21
11.2	LAN VoIP	21

1 Introduction

The Allworx® 10x Server is designed to meet the communications and networking needs of the typical small business, while also simplifying the setup and maintenance of the IT infrastructure for the business owner. The problem is that the typical small business is not always so typical and the landscape of protocols, providers, and terminology can be somewhat overwhelming.

This paper is intended as an explanation of key networking fundamentals for the small business owner who is considering an Allworx 10x. An understanding of the decisions and configuration options should improve a non-technical owner's control and effectiveness as s/he establishes a workable infrastructure that meets the needs of the business, today and tomorrow.

2 The WAN Interface and your Internet Service Provider (ISP)

Allworx provides simple and secure access to the Internet for users on your company's Local Area Network (LAN). This capability is sometimes referred to as "Internet Connection Sharing," since there is a single Internet connection shared by all LAN users, rather than individual connections. In this role Allworx acts as your local networking router. While you won't need to purchase any other equipment to get connected to the Internet, unfortunately Allworx [like other network systems] can't get to the Internet by itself; you will also need the services of an Internet Service Provider (ISP) to actually physically connect to the Internet.

Connecting to the Internet or any other external network is the role of the Wide Area Network (WAN) interface of your Allworx unit. Generally, when you set up Allworx to share your connection with all the PC's on your LAN, the Allworx WAN interface is used to hook to your ISP provided modem or router. Allworx is designed to look like a single ordinary PC when connecting your LAN to the Internet and should work with any ISP service provider equipment that allows you to hook to the Internet using a standard 10/100 Ethernet cable between Allworx and the ISP provided equipment. This includes just about any Cable Modem, DSL modem or T1 based services that use standard TCP/IP networking between you and the ISP.

When configuring your Allworx system for Internet access, you will need to know the following from your ISP provider:

- Static IP Address or Dynamic (DHCP Client) IP Addressing
- DNS Server IP Address(es)
- IP Netmask and Gateway Settings

When your system is being installed and set up, your system administrator or consulting installer will enter these addresses and settings in the system 'Network Settings' segment of the Allworx Administrator web page.

To give you some idea of the significance and background to these settings, the following sections are offered as a brief tutorial.

3 IP Addresses, Netmasks, Gateways

All computers that connect to the Internet using the TCP/IP protocol have to be configured such that each computer on the Internet knows how to locate every other computer on the Internet. This is done with a unique set of network settings which consists minimally of an Internet Protocol (IP) Address, a Netmask, and a Gateway Address. The IP address gives the PC or server [host in networking terminology] a unique identity on the Internet so that when any computer wants to send data to it, it knows where to find it. It is sort of like a Social Security number for computers. That address must be unique for every computer on the Internet so that data sent on the network gets to the right place.

Most people somewhat intuitively understand IP addresses so we won't spend lots of time on that. Suffice it to say that the IP address of each and every host must be unique on the Internet so that traffic knows where it is going. On the other hand, the terms netmask and gateway go beyond many people's knowledge of networking. Fortunately, the concepts are simple and the early engineers of the Internet did a great job of making the roadmap of the Internet easy to follow. In short, netmask and gateway give each host a way to find any other host on the Internet and form the basis for *routing* decisions on the Internet

When a host wants to send a packet of data to another computer, it needs to know how to find that computer. Fortunately, the decision is simple and can be answered with one simple question: "Is the host I want to talk to *local* or *remote*?" The Netmask is used to figure out the answer to this question. The host uses its own IP address, the destination host IP address and the netmask to determine if the desired location is *local* or *remote*. If the answer is *local*, then the packet is sent directly to the destination via the LAN's hub or switch using the physical *MAC* address of that computer. If the answer is *remote*, then the host is needs to activate the services of a *router* to forward the packet along to its destination. How does the host find a router to do this? The Gateway is the IP address of the necessary router for your LAN.

How do I know what the right IP, Netmask, and Gateway Settings are for my Allworx unit? – Good Question! – Since Allworx typically acts as both a router and a host, there are actually two sets of settings (WAN and LAN) for the Allworx unit with the gateway address always being the same for both sets of settings. For the WAN interface, they will be provided by your ISP or set automatically via a protocol called DHCP (discussed more later). For the LAN, generally the factory defaults will be sufficient.

Note: All controls for these configuration options are on the Network Settings page of the Allworx admin tools.

4 Allworx Networking Security - Firewalls and NAT

As a *complete* solution for your IT infrastructure, Allworx includes enterprise class Firewall security and TCP/IP routing functions to support moving (or blocking!) traffic between the private LAN and Public WAN interfaces of your Allworx unit. The Allworx Firewall, routing modes, and Network Address Translation (NAT) all go hand in hand to provide this capability. We've built in a wide range of options designed to support a variety of typical small business networking setups.

Note: All of these options are configured on the Security Settings" page of the Allworx Networking administrative area.

Because of the advanced capabilities available, this particular topic can get very involved. The Allworx unit is intended to be as flexible as possible in this area to meet various demanding applications typical of more complex environments, without getting too complicated for the average user. To start the conversation, let's get some definitions out of the way:

4.1 Firewall

Most people have heard of firewalls, but what do they really do? In brief, they protect your private LAN network from external access by unwanted traffic. At a lower level, a firewall is a special type of network router. Normal routers follow all the normal Internet TCP/IP network routing rules without regard to security concerns, while a firewall introduces *policy* on the routing decisions above and beyond the original rules of Internet traffic. Generally, these policy decisions are based on the IP addresses involved in the transaction and the physical interfaces the packets are coming from or going to.

In the context of Allworx specifically, the physical interfaces are the LAN and WAN interfaces of your unit. When the Allworx firewall is enabled, by default, all internal LAN traffic is allowed Internet access to the outside, but nobody on the Internet is allowed access to your LAN. In fact, the Allworx Firewall is the most powerful form of Firewall – The Stateful Packet Inspection (SPI) filtering Firewall, for maximum system safety at all times.

4.2 Network Address Translation (NAT)

As discussed in a previous section, we stated every *host* on the Internet must have a unique IP address. This is not entirely true. A more correct statement would be to say that every host on the Internet must appear to have a unique IP address from the point of view of the Internet. This is a subtle but important distinction. NAT allows multiple hosts on a LAN to share a single public IP address. Using NAT solves several potential problems:

- IP Addresses are running out. There are many more computers that have Internet access than there are IP addresses to go around...amazingly enough!! While there are theoretically 4-billion IP addresses to go around, certain technical factors that simplify routing decisions waste lots of potential addresses. This makes a *public* IP address a valuable commodity that costs money.
- Most ISP's only provide you one IP address as part of your service (perhaps up to five for "free") and additional ones are typically rented on a monthly basis. NAT allows you to have more hosts on your LAN than public IP addresses. With Allworx as your NAT/Firewall, you only need one public IP to give all your computers on the LAN access to the Internet!
- Public IP Addresses have to be maintained as unique and routing tables must be updated at your ISP when things change or move around. NAT enables the use of private IP address ranges that you can

manage and change on your own without permission or support from your ISP. In the case of Allworx NAT capabilities, it will manage the private addresses for you automatically!

- Public IP addresses provide an address for hackers to attack. NAT hides the true IP address of hosts on your LAN under a single public address, making it harder for hackers to understand things about your network. NAT alone does not replace a firewall. However, NAT combined with a Stateful Packet Inspection Firewall provides added security. Allworx provides this additional level of security: when the Allworx Stateful Packet Inspection Firewall is enabled, NAT is automatically enabled as well.

4.3 Mode Summary

With the definitions out of the way, we will explore the various security modes of your Allworx unit and explain what each mode is:

- LAN only Mode – This mode is used when the WAN interface of Allworx is not needed. In this mode Allworx works like an ordinary LAN host and typically provides no routing, NAT, or firewall functions since all traffic is bound to the LAN interface only. If Allworx is configured as a DHCP server (see DHCP later), it will assign a netmask and gateway to hosts based on its own LAN interface netmask and gateway settings.
- Router Mode – This mode is used when Allworx is used as an ordinary two port router with the Allworx providing the routing functionality between the LAN and WAN interface. This mode is typically used when your LAN addresses need to be public or when the WAN interface is connected to another internal sub-network. The firewall and NAT is always disabled in this mode. If Allworx is configured as a DHCP server, Allworx will assign itself as the LAN gateway to the WAN.
- Firewall/NAT Mode – This mode (by default) makes the LAN completely secure from the WAN interface and only outbound connections are allowed from LAN to WAN. In addition, all traffic from LAN to WAN and back is translated through the NAT mechanisms to allow sharing of the Allworx WAN IP address with all hosts on the LAN. Connections from WAN to LAN are always refused, by default configuration. However, when desired, specified LAN devices can be made visible on the WAN. Note: Allworx's own public services are still directly available on the WAN, but the LAN side services (intranet, admin, etc). are fully secured.
- Firewall/NAT/DMZ Mode – This is identical to the previous mode, except the firewall mechanisms are also applied to Allworx's own public WAN interface. As a result, your unit is more resistant to various forms of known Internet attacks, such as denial-of-service type attacks. Your LAN is always protected when the firewall is enabled, but DMZ mode increases protection for the Allworx external WAN interface. With DMZ enabled, you can selectively control which WAN protocol *ports* are even visible on the Internet. This is sometimes referred to as a "stealth mode."

5 Dynamic Host Configuration Protocol (DHCP)

There is usually much confusion over DHCP. This is particularly ironic because the DHCP protocol is intended to make the life of the users and administrators easier. While the protocol is quite involved, what it does is actually really simple to understand. The confusion arises because of the notion of DHCP client and server modes. Let's clear this all up now!

Recall that all *hosts* on the Internet have to have a unique IP address, a *netmask* and a *gateway* setting to participate on the Internet. Historically, this was all set manually on each computer when the operating system is installed and the host is placed on a network. This is referred to as "static IP addressing". This creates two potential difficulties, one for the end user and one for the administrator:

- For the administrator this means every computer has to be configured and maintained manually. A network or ISP change may affect every computer on the network and each would have to be updated by hand, separately!
- For the end user they can't relocate a computer to other networks without manually re-configuring each time. For a desktop PC this is potentially not a concern, but for a laptop computer you move between offices or work and home...it's a real inconvenience!

The DHCP protocol addresses these problems through two pieces of software.

- 1) A DHCP server program maintained by the network administrator; and
- 2) A DHCP client program that is usually part of the operating system for any network driver/adaptor.

Using DHCP and the laptop computer example you simply plug into any network drop and once Ethernet link is acquired the DHCP client automatically queries for the local DHCP server on the network who then answers the client's query and automatically provides the correct settings for that particular LAN. IP addresses are still unique to each computer, but they are maintained in a pool and re-circulated, as needed, using *leases*.

There is only one real drawback to DHCP – Your IP address can change over time! This is especially true when you turn off your computer for the *lease* duration or if you have a laptop and it moves around between networks often. While this is not generally of concern for a regular PC or laptop this is a problem for servers, especially public ones! You want to always have people find your servers at a known "address". This facilitates the need to still maintain tables of "statically assigned" IP addresses.

Relative to Allworx, because of its extensive breadth of capabilities it can provide the role of both DHCP server and DHCP client, simultaneously, depending on the particular application. The DHCP server mode applies to Allworx providing the DHCP service to computer hosts on your private LAN. While the default settings of the Allworx DHCP server are generally sufficient, there is quite a bit of control over its behavior, including disabling the server. These settings can be manipulated through the "Servers – DHCP" page of the administrative tools. Note there should only be one DHCP server enabled per LAN network.

To make the DHCP server as seamless as possible, most settings the DHCP server provides to LAN clients are determined automatically for you! This is one of the ways Allworx simplifies configuration and setup of your network. However, for the more curious or technically inclined, we'll describe how Allworx decides what values to assign:

- IP Address – The IP Address is always a LAN address from the available pool. Allworx defaults to assigning addresses from the dynamic range of "1" through "100" on the LAN subnet, skipping its own address if it overlaps. This range can be adjusted on the DHCP server settings page if desired. Allworx will assign addresses for up to 254 hosts on the LAN.

- Netmask – This is always directly inherited from the Allworx LAN netmask setting and assigned accordingly.
- Gateway IP – The gateway setting is delivered as Allworx's own IP address when Allworx is configured as a network firewall or as a router. However when Allworx is configured in "LAN only mode" this setting is directly controlled by Allworx's own gateway address, entered on the Network Settings page.
- DNS Server IP – The DNS server IP address given out is delivered as Allworx's own IP address when Allworx is configured as a network firewall or as a router. However, when Allworx is configured in "LAN only mode" this setting is directly controlled by Allworx's own primary DNS server IP address, entered on the DNS Server settings page.
- Default Domain – The domain is always driven from the domain setting entered on Allworx Network Settings page.
- Time Server – If the host on the LAN requests time services, Allworx will always provide its own IP address as the LAN time server.

The Allworx DHCP client side functionality applies to Allworx's WAN port only. With the Allworx DHCP client service enabled, Allworx can automatically configure its own WAN interface through a separate DHCP server available on the WAN interface. This DHCP server would generally be maintained by your ISP and is very common with lower cost Internet services where a static IP address is not provided. Allworx will automatically configure its own WAN IP Address and Netmask from the external DHCP server.

Note: For security reasons, the Allworx Domain Name and DNS server IP address settings must always be entered manually by the administrator.

6 Domain Name Server (DNS) and Domain Names

So far, we have primarily focused on IP addresses as the identifying address of hosts on the Internet. While this clearly is the foundation of all networking configuration and routing, IP addresses are not very friendly to the end user. After all, do you know the IP address of www.inscitek.com or even www.amazon.com. Of course not! The role of DNS is to provide the mechanism for friendly names to be available to identify hosts so only the administrators of the various sites have to know the real IP addresses. Not only is this easier for everyone involved, but it also allows the underlying IP addresses and computers to change over time without having to manually inform everyone about the change. A simple DNS server update will take care of it for you.

If you think about it, DNS is really the engine that makes the Internet work. It is a massive distributed database maintained individually by each domain name owner to allow a mapping of both public and private names to their current IP address. It is not unlike the phone book for each area code or municipality. DNS is also integral to Internet Mail routing, knowing where to send email directed to particular domains.

Much like DHCP, there are two different parts to DNS:

- The DNS server acts as part of the massive world-wide database, holding one piece of the *namespace* and
- The DNS *resolver* acts as the client tool, and knows how to look things up in that distributed database when you type <http://www.amazon.com> in Microsoft Internet Explorer.

Also, like DHCP, Allworx can provide both the *server* and *resolver* services to your LAN. In fact, when Allworx is configured to be your DHCP server and the DNS server is enabled as well, Allworx will automatically point your PC's to use the Allworx DNS *resolver* and *caching* capabilities, speeding your access to the Internet.

To get DNS going on Allworx is reasonably straightforward. For your LAN to be fully serviced by the Allworx DNS capabilities, you simply need to specify the name of your local domain such as "mycompany.com" and specify the IP address of your ISP's DNS server which they can provide for you. Both of these items are configured on the Network Settings page of the Allworx Admin Tools.

While it is not uncommon for your company's domain name to be hosted externally by your ISP or other provider, Allworx also has the ability to host your domain to the World Wide Web for you. This is particularly useful if Allworx's public web server features are being used and you don't want to pay a provider to host the domain name for you. You simply have to tell your Registrar of your domain name the static IP address of your Allworx, as provided by your ISP.

Note: Static IP addressing is required for the Allworx WAN interface when hosting your own domain. Otherwise people on the Internet won't know your Internet address.

6.1 Settings Summary

To help clarify the functionality of DNS services in Allworx, let's describe in more detail exactly what you enter in the DNS server setup page and exactly how the values are used:

- Primary DNS Server – This IP address is the server that Allworx contacts to resolve DNS lookups for its own use. Typically this setting is provided by your ISP, but it can be the address of any trusted DNS server and may be a LAN IP address if you are running a separate DNS server of your own.

Note: This setting should always be set for proper operation of Allworx and is very important for proper mail operations when Allworx is being used as an SMTP mail server. In addition, all hosts on the

LAN need this setting to be properly set when those clients are configured to obtain their own settings from Allworx's DHCP server.

- Secondary DNS Server – As the name implies, this is the alternate DNS server to reference when the primary server is not available. This setting is optional, but improves robustness in times when the primary server is down or overloaded. If you don't have a valid secondary server to reference, this field should be left blank. I.e.: Do not leave invalid DNS server IP addresses in this field.
- Enable Use of Primary and Secondary DNS Servers – This setting is a checkbox option. Generally, this item should always be checked for normal operations when Allworx is connected to a network. When the option is left unchecked, Allworx operates in a stand-alone type mode where it assumes it is not connected to a network or the Internet and never attempts to resolve DNS requests to an external server. Additionally, and most importantly, all requests made of Allworx as a DNS server which it can't resolve internally are reported as *non-existent* names/domains in an *authoritative* manner. This mode of operation enhances performance when only a few PC's are tied to Allworx and there is no connectivity to the outside world; rather than experiencing lots of DNS lookup timeouts, hosts will quickly come to the conclusion that the desired destinations are in fact not-reachable.

Networking Tip:

DNS is often overlooked during network troubleshooting. When you are having networking difficulties, always be sure to confirm proper operation and settings relative to your DNS setup. Almost all networking facilities depend on DNS and very bizarre behaviors can result when DNS is improperly configured or stale data is cached in a referenced DNS server.

7 Mail Configuration and Unified Messaging

The mail transport and delivery aspect of your networking infrastructure can be more complicated than previous topics. This is true for two reasons:

- Mail depends on all the previously described facilities being configured and working properly, and additionally introduces a few new protocols of its own.
- There are lots of choices available concerning exactly how you want to configure things for email delivery and there is no one right answer for all circumstances. The best option depends on the exact circumstances.

Not to worry, however! With email, ISP's and mail tools being so common today, most people have heard most of the terms. We just need to fill in some details and paint the complete picture to help you on your way. If you have made it this far and are following along pretty well, then you should be able grasp most of the concepts here without a problem. So let's start off first with some background definitions on the two primary protocols associated with email on the Internet:

- **SMTP** – This somewhat arcane protocol acronym stands for Simple Mail Transport Protocol. SMTP performs the basic mechanism for delivering email from point A to point B over the Internet. If you have a mail client and need to send mail to another location, you typically have to specify an SMTP server name or IP address that will be used for mail transport facilities. However, SMTP is not only used by your mail client to get the message on its way to the SMTP server you specified; it is also used for each server *hop* the message makes along the way to the destination *mailbox* of the intended recipient.
- **POP3** – This protocol is a little misleading in its naming. The POP3 acronym stands for Post Office Protocol, version 3 and implies an operation that parallels what the postal service would do to deliver messages. However, that is what SMTP does. In any case, POP3 comes into play where SMTP stops. While the job for SMTP is to get the email to the destination mailbox on the server where your messages collect, POP3 is about moving your email messages from that server's mailbox to your desktop client software's inbox. In this regard, POP3 might have been better named POBP for "Post Office Box Protocol" but that doesn't quite roll off the tongue as well.

With the basic definitions in hand, you need to decide how you want to set up your mail flow. Keep in mind that Allworx implements and will support a wide variety of configuration in this regard, including all the configurations described here, and more! Consider the following items as we move through this discussion:

- **Inbound Message Delivery** – When mail is sent to you from out on the Internet, where do you want it to go? Do you already have your domain and mailboxes hosted by an external service, running on an existing internal mail server or will you be switching to using the Allworx set of messaging facilities?
- **Outbound Message Delivery** – When you push "send" in your desktop mail client, what SMTP server do you use for delivery services? Sometimes this is provided by an ISP, and sometimes this is already an internal server or is again being transitioned to Allworx. One thing to keep in mind is that using an internal server (Allworx or otherwise) for support here is helpful for message security and privacy for messages exclusively being distributed to local users at your business.
- **Unified Messaging** – The Allworx Voicemail and FAX capabilities deliver messages to each user's Allworx mailbox. However, if Allworx is going to be used in parallel with other mailbox(es), you need to decide how this new source is going to be integrated with the others. Again, there are multiple options here as well.

The first decision to make is whether Allworx will become the user's primary mailbox or not for inbound email from the Internet and from other local users. Certainly, having Allworx provide the primary mailbox service is generally preferred, but in many existing installations it may not always be practical to switch from a legacy setup, at least initially. The next section details the options and features to consider when Allworx is the primary mailbox and the following section details the options you have when you wish to stick with an existing setup.

8 Allworx as the Primary Mailbox

From a clean sheet view of your network, selecting Allworx as the users' primary mailbox is generally the best option. However, considering legacy systems and processes already in place within your company, this option may not be the path of least resistance to integrate Allworx unified messaging features into your environment. This may be especially true if you already have a sophisticated environment incorporating a Microsoft Exchange server, for example. On the other hand, if you wish to take maximum advantage of Allworx's own group collaboration capabilities and value adding client software it will probably be worth the effort: your recurring costs savings will be significant, for both licensing and ongoing support requirements.

8.1 Inbound via SMTP

Relative to inbound email delivery from the outside, Allworx is fully capable to act as an SMTP server to receive mail directly from the Internet and deliver it to local mailboxes. This choice makes sense when you have a reliable Internet connection of sufficient bandwidth that is typically available 24/7 at a static IP address. If your Allworx WAN port will not be connected to the Internet all the time or you are using dynamic IP addressing, you probably want to consider a different option described below.

In this mode, by default, mail from the outside is only accepted for local deliveries to internal mailboxes to prevent hackers from spamming other sites through your Allworx unit. However, this type of mail *relaying* can be enabled, if desired.

Note: Allworx always supports mail relaying via SMTP from LAN clients so that all LAN clients can use Allworx as their SMTP server to insure security and privacy of mail between local users.

For inbound delivery to work correctly to Allworx from the Internet, a mail exchanger "MX" record has to be configured to point to Allworx under the DNS *zone* for your domain name that Allworx is configured to support. This mechanism under DNS is how mail servers on the Internet know where to deliver email for your domain. If you are also using Allworx to host your domain name for the Internet, Allworx automatically configures the proper MX record and no additional setup is required. However it is not uncommon for your domain to be hosted externally at the *registrar* for your domain or through your ISP. In this case, you need to request an MX record be setup that points to Allworx for mail delivery.

8.2 Inbound via POP3

If you don't have a highly available Internet connection or are already using another server either internally or externally provided by an ISP to receive email from the Internet, then the POP3 client capabilities of Allworx can be very helpful. Using POP3 client mode, Allworx can automatically poll other mailboxes via POP3 to download email into the local Allworx mailboxes. Allworx supports individual POP3 accounts for each user and a single external POP3 account common to all users.

On the user administration page for each user, Allworx can be configured with server and account information for one or more POP3 mailboxes that will be automatically downloaded from on a periodic basis and used to populate that user's local mailbox. All messages downloaded in this matter, no matter how they were originally addressed, are delivered to the associated user's mailbox.

The user administration page for the Allworx system admin account has the same features except this POP3 download capability behaves differently. For POP3 accounts associated with the admin user, each downloaded message is analyzed for addressing information and when local mail addresses are discovered corresponding to local users, that message is automatically delivered to that user's mailbox. This feature is very useful when

you are paying only for a single mail account at your ISP and all messages, no matter what user they are addressed to, are delivered to a single common mailbox at the ISP.

Note: In this mode, if none of the addresses are for local users, then the admin user itself receives the email message. Also note that email aliases added on the system messages alias pages are also considered. This allows messages addressed to virtual users or groups such as “support” or “sales” to go to a specific user or list of users.

8.3 Mailbox Access

With Allworx acting as the primary mailbox, regular email messages and unified voicemails and/or Faxes are directly available in a common location. Using the Allworx Communication Center software as the desktop client, configuration will be completely automatic based on automatic server setting discovery and the user login process on that client.

Support for other clients that support POP3 mailbox access, such as Microsoft Outlook and Outlook Express, is seamless as well. For these 3rd party tools you simply need to add an account that specifies Allworx both at the POP3 server location for incoming mail and Allworx for the local SMTP server. Allworx has fully integrated POP3 server support to allow such tools to download messages from the server’s mailbox into the client’s inbox. The POP3 service is made available to LAN and to the WAN port if enabled through the firewall. This allows email to be fetched from the office or while on the road from a laptop.

9 Allworx as a Secondary Mailbox

This mode of operation comes into play when another mail server is going to continue being used as the primary location for the user's incoming and outgoing email. In fact, in such situations it is possible to completely ignore Allworx mail capabilities and stick with what you already have without any impact on your existing infrastructure. However, many businesses want to take advantage of Allworx's time-saving unified messaging features related to Voicemail and FAX delivery to the user's regular inbox, which is still possible even when used in conjunction with other mail servers.

Before we dig into the options here, it will be useful to explain some background. It is important to understand how Voicemail messages are delivered and accessed via Allworx. Recall that Allworx provides the capabilities to access your mailbox both from the telephone and from the network. As a result, when voicemails are left for you via the phone system it is important that they remain available within the Allworx mailbox so that they can still be retrieved from the telephone. This requirement eliminates the blind forwarding of the voicemails to another location since it would no longer be available over the telephone. This means you have to accept delivery of the Voicemails to more than one location (Allworx mail, plus the primary mailbox) or you have to configure the desktop mail client to check for messages in both locations. Either option is available and are explored further here:

9.1 Pull Model: Unified at the Client

Using the features of most email clients including Microsoft Outlook and Outlook Express, you can configure those tools to download messages from multiple locations. Everything will appear in one inbox, but it is the client that unifies messages from your primary mailbox and the secondary Allworx mailbox. The POP3 protocol is used in a 'download only' mode to populate the inbox, with the additional messages going into the Allworx mailbox. However, it is important to configure the POP3 support in the mail tool to still "leave a copy on the server." Otherwise downloaded messages will no longer be available via the telephone since they would have been deleted from Allworx by the mail client. Additionally, most email tools have an automatic "delete message after X days features" to automatically cleanup old voicemails that maintain on the Allworx mailbox.

9.2 Push Model: Replicated by Allworx

In this model, Allworx is configured to deliver the incoming voicemail messages to your Allworx inbox and also deliver a second copy to the primary mailbox. This is accomplished via setting up a mail alias on the Message Alias configuration page of Allworx. Using this technique you setup a somewhat odd looking alias for each user operating in this mode:

```
username = username primaryname@primarydomain.com
```

In short, an alias is setup named the same as a local user and you specify that the name maps to that same username and additional make that alias map to the address of the primary mailbox address. Using this type of alias rule, Allworx will deliver the message to the Allworx mailbox for the user making the messages available via the telephone and also send a copy of the message to the user's primary mailbox located on another system.

In this mode of operation it is important that the other mailbox [the one receiving the delivery] can be found from Allworx's view of the network. If Allworx itself has access to the Internet from either its LAN or WAN interfaces, typically this will be a valid assumption. However, if Allworx is isolated from the Internet, it is important that its DNS setup be configured such that Allworx will be able to resolve the user's mail address through MX record lookups and the server(s) identified therein are reachable by Allworx.

10 Advanced Topic: Using Allworx to host your DNS Domain

Allworx has a fully integrated DNS server as part of its standard functionality. This DNS server can be thought of as filling two independent roles:

- LAN Support – In this role client PC's on the LAN point to Allworx and use Allworx as the primary DNS name resolver to convert domain names into IP addresses. This mode of operation has two important benefits. The first is performance since Allworx will cache common lookups and make them immediately available to local users without having to go over the WAN interface to the ISP's server. Secondly, Allworx automatically incorporates local knowledge via DHCP operations to be able to resolve the names of local computers for other people on the network. This is sometimes called Dynamic DNS support. Additionally, Allworx has useful names available to the local users to be able to access the various facilities of Allworx without having to use IP addresses manually.
- WAN Support – In this role Allworx acts as the DNS server to the Internet for your domain, providing the public definitions of how to navigate your domain. For example, all requests related to your domain name whether they are email lookups for mail going to your site or IP address lookups for people coming to your web-site, etc. Allworx is used as the authority for your domain.

Allworx is fully capable of supporting both roles and this is one of the advantages of choosing Allworx. While LAN support of DNS services almost always makes sense if you don't already have another DNS server configured, using Allworx as the WAN side public DNS server may not always be a good choice. This fact is independent of Allworx and has more to do with the robustness of your connection to the Internet.

When hosting your domain locally, it is very important to maintain a very reliable Internet connection with sufficient bandwidth to service all outside requests. Additionally, it is generally recommended that you have at least two servers hosting your domain for redundancy. If your Internet connection is down or your DNS server is taken down for a specific reason, your domain doesn't necessarily exist for that period of time, and incoming email starts to bounce, your web-site is not available, etc. For these reasons, DNS hosting, specifically, of your domain can generally be more reliably and cost effectively hosted by either your ISP or your domain registrar's servers. They have the bandwidth, redundancy, and support staff to maintain a highly consistent DNS presence.

In any case, should you choose to public host your domain name directly on Allworx, this additional set of information should prove useful to people with detailed knowledge of DNS topics:

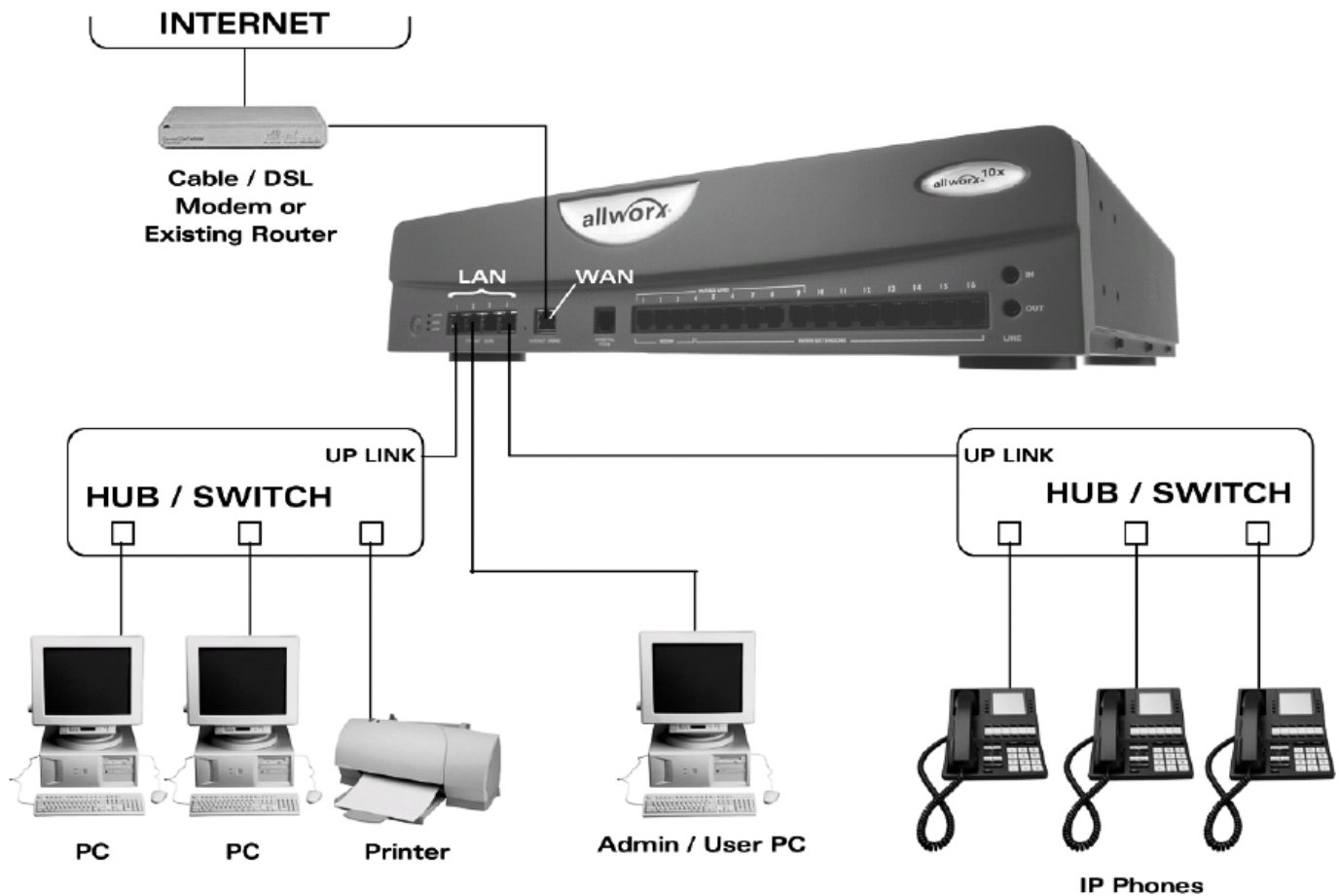
- The Allworx DNS server currently has configuration support for a single DNS zone. This zone starts at the domain name specified on the Network Settings page and encompasses all names at or below that name in the namespace. In other words, there is no way to specify delegate sub-zones off of Allworx. Of course, Allworx itself can be implemented as the sub-zone to the primary domain by simply configuring Allworx's domain as the domain server for a lower level domain name.
- Allworx makes no distinction between internal lookups and external lookups. Names added for internal addresses are available from the outside as well, even though those names may not be routable from the Internet. This was done to support VPN features seamlessly so that external users have the same names available as internal users without the need for complicated DNS configurations to be defined and maintained.
- DHCP Server operations of Allworx are automatically tied into the DNS entries. Each host that gets a DHCP address from Allworx and provides a local hostname will cause that name to be available from the DNS services. Additionally, as these hosts come and go on the LAN and/or IP addresses change, the DHCP server automatically keeps the DNS up to date in a dynamic fashion. Entries are also

scrubbed from the DNS server if the DHCP server expires a lease of such hosts and they are not available to renew those entries.

- The MX record for the Allworx SMTP server for inbound access is automatically created to map to Allworx's own interfaces. This is intended to support inbound email from the LAN or WAN side without manual configuration.
- Allworx has several built-in entries that are automatically configured as part of the server's normal network settings. These virtual host names each map automatically to either the WAN or LAN IP addresses of Allworx. Additionally, static address record mappings can be manually added to the DNS name space as desired. This is configured by adding such entries on the DNS Server configuration page. The built-in names are listed here.

www	WAN IP Address – Intended for access to the Allworx publicly hosted website.
corp	LAN IP Address – Intended for access to the Allworx privately hosted Intranet website.
admin	LAN IP Address – Intended for access to the Allworx system administration website that is available at port 8080.
lan	LAN IP Address – Specific mapping to Allworx LAN IP Address
wan	WAN IP Address – Specific mapping to Allworx WAN IP Address
smtp	WAN IP Address and LAN IP Address – Mapping for inbound SMTP service from either the LAN or WAN for 3 rd party mail tool access
pop	WAN IP Address and LAN IP Address – Mapping for POP3 mailbox access from either the WAN or LAN

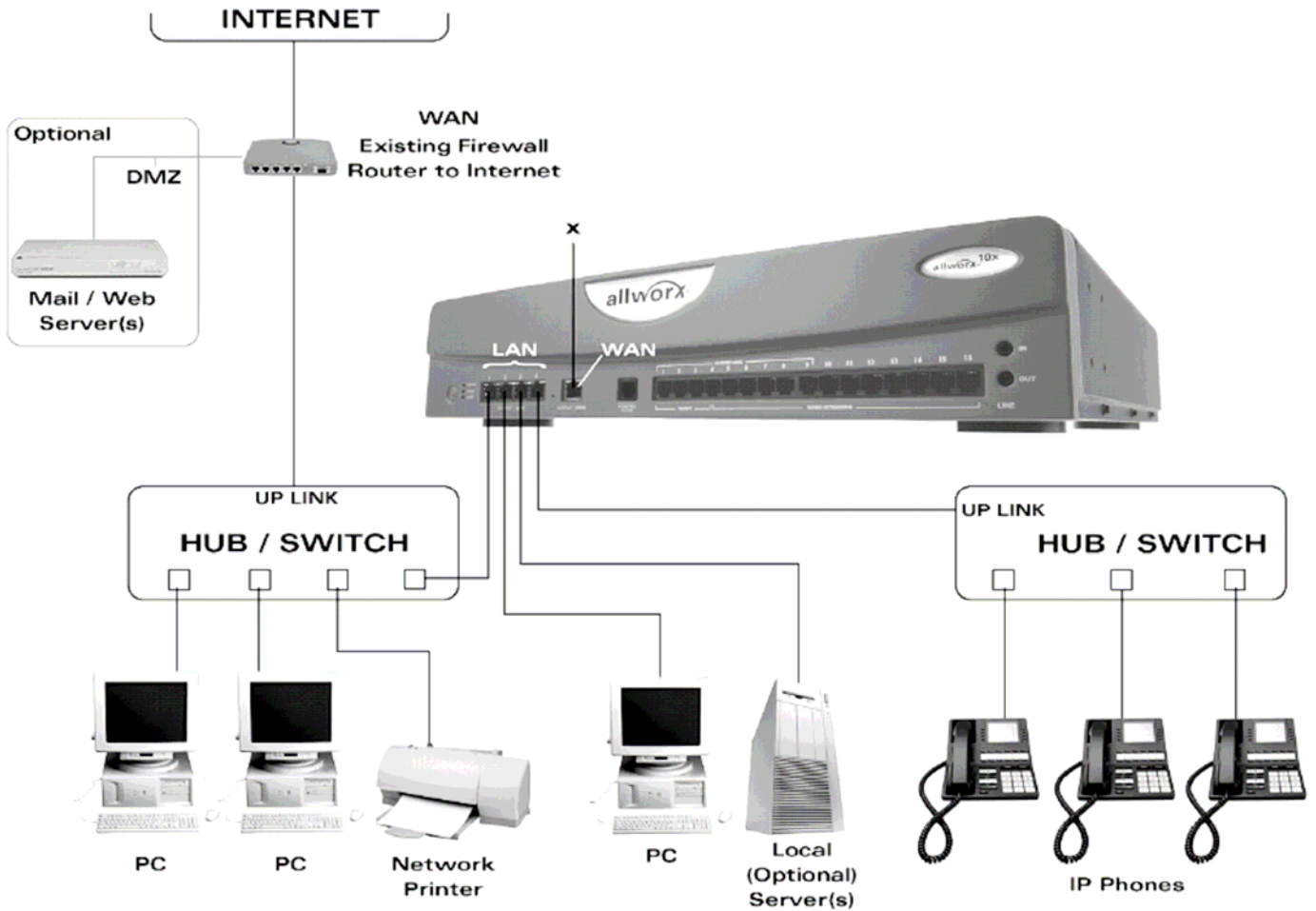
Allworx Preferred Setup



Allworx Provides: (Typically)

- Firewall Support and Router - **Yes**
- DHCP Server - **Yes**
- DNS Server / Cache - **Yes**
- Mail (SMTP) Server - **Yes**
- Web Server - **Yes**

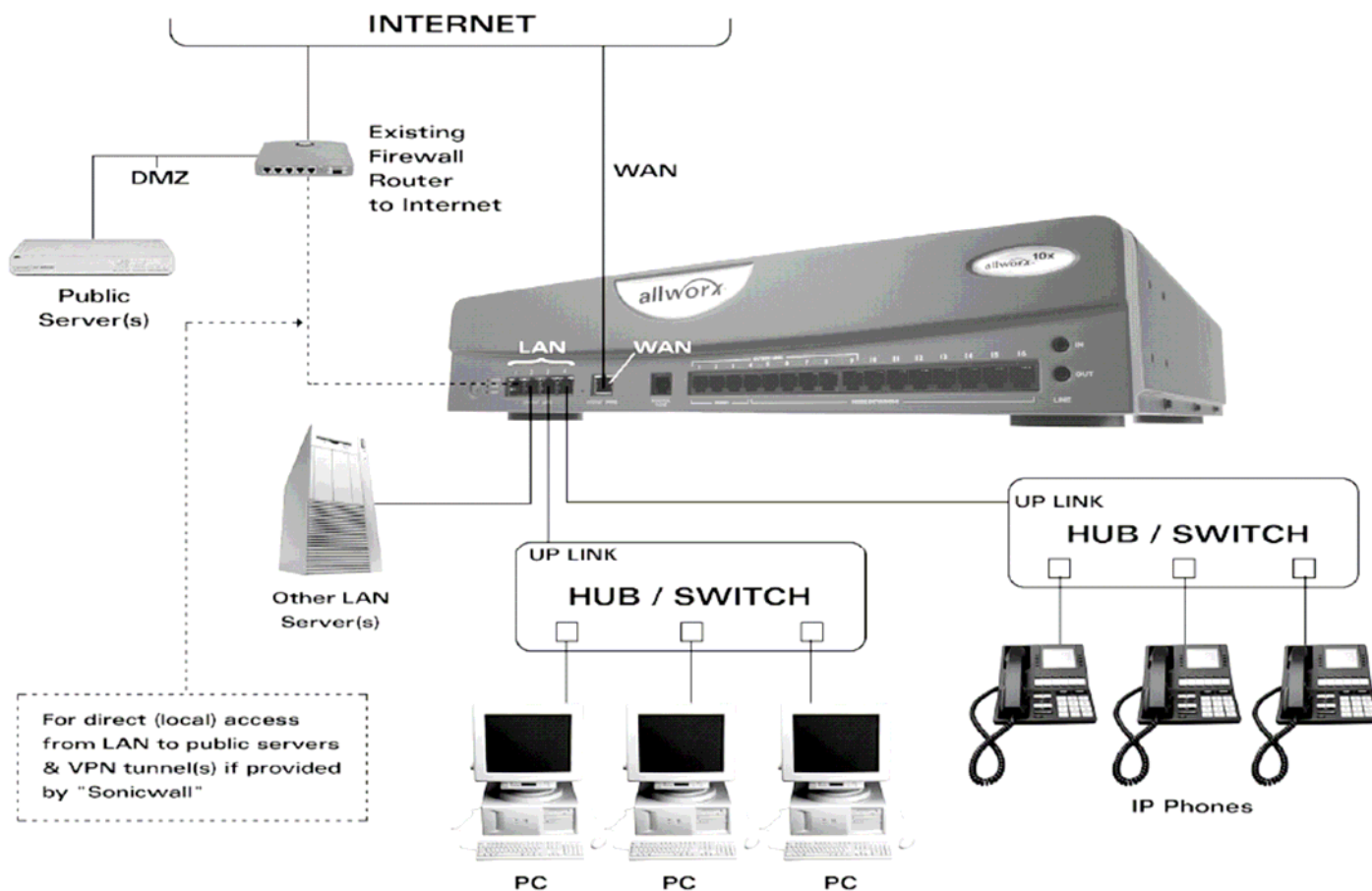
Allworx Alternate Setup (1)



Allworx Provides: (Typically)

Firewall Support and Router - **No**
DHCP Server - **Yes or No**
DNS Server / Cache - **No**
Mail (SMTP) Server - **Yes or No**
Web Server - **No**

Allworx Alternate Setup (2)



Allworx Provides: (Typically)

- Firewall Support and Router - **Yes**
- DHCP Server - **Yes or No**
- DNS Server / Cache - **Yes**
- Mail (SMTP) Server - **Yes**
- Web Server - **Yes or No**

Advanced Topic: General SIP and Soft Phone Support

Allworx has fully integrated support for Ethernet based IP Telephones using the SIP Protocol as described in Internet Standard RFC-3261. Allworx uses the G.711 coder under RTP/UDP/IP for LAN communications of real time voice data. Generally speaking, any SIP-based physical or soft phone compliant with the standard should function from a basic call handling perspective with Allworx. However, configuration and setup can get somewhat involved and not all features of a given phone brand may work as expected. Additionally, dialing rules may vary significantly from phone to phone.

InSciTek maintains a list of officially supported phones that we test against the Allworx server. Phone models not on that list generally will work, but are not supported by InSciTek and typically will not automatically configure without manual intervention by the administrator of the system to configure both Allworx and the phone itself.

11 Advanced Topic: IP Telephony and Quality of Service Issues

A common question relating to the use of IP telephones on a network is a concern over Quality of Service (QoS) issues. QoS is a widely applied term and is loosely applied to both traffic prioritization techniques and protocols for reserving and managing bandwidth. Here we talk about QoS as it applies to overall perceived voice quality. In most situations, this topic only becomes a concern when Voice over IP (VoIP) traffic has to be managed across multiple networks where there are one or more intermediate routers between end points and the bandwidth between those end-points is less than the bandwidth available at either end point network. For the sake of reference here, we call that mode the WAN VoIP case. The more typical Allworx case for a single site without any internal routers only has to consider the much less complicated LAN only VoIP case.

11.1 WAN VoIP

A full discussion of the WAN VoIP telephony issues is well beyond the scope of this document. Specific to Allworx, the assumption is that VoIP traffic is local to the LAN or is going between two sites maintained by an Allworx voice tunnel using Allworx's multi-site features (VPN) available in the June, 2003 time frame. In this situation, InSciTek has done the hard part for you as long as Allworx is the router sitting between the LAN and WAN at each site. The only thing you have to insure is that your ISP can guarantee enough bandwidth between sites to support the maximum amount of configured voice traffic between those sites. For complete information on this, consult the Allworx "Sites" page of the VPN administration page and associated documentation.

For a detailed understanding of this topic, InSciTek recommends consulting one of the Cisco IP Telephony books. They do an excellent job of exploring the proper engineering of complex WAN networks containing voice traffic.

11.2 LAN VoIP

On a single LAN, QoS issues are not generally a concern, and most ordinary low-cost switches and hubs can be used to connect both computers and IP phones to the network without concern. Understand that Ethernet and IP protocols are inherently designed with the necessary fairness and flow control mechanisms to allow VoIP traffic to work well within the LAN environment of a single subnet. The exception to this is when there is excessive broadcast traffic or an improperly configured device is saturating the LAN in an uncontrolled manner, thereby causing non-trivial packet loss.

The key thing to remember here is that no protocol reservation technique or buffer priority technique is really going to fix a poorly engineered network that is constantly being overloaded. The source of the problem must be addressed first. A well-engineered LAN that is efficiently handling data already should not have any issues supporting the additional VoIP loading w/o any specific QoS protocol support or custom VLAN configurations. On the other hand, if the network is really close to saturation, you really need to think about re-engineering the network to address the problem. This will fix the data transfer performance problems and allow VoIP telephony support to work as well.

The most conservative approach recommended with Allworx is to dedicate one of Allworx's 4 switched LAN ports to IP telephony. In this configuration, all the IP phones either plug into Allworx directly or all hang off the same switch/hub that is connected directly to Allworx. The other devices on the LAN then plug into separate sets of switches/hubs that hang off one or more of the other switch LAN port(s) on Allworx. Since Allworx will automatically manage the traffic across its own switch, keeping the data and IP traffic on separate switched ports on Allworx will ensure proper operation in almost any circumstance.

If you choose to go with a more distributed approach of mixing IP phones and other LAN devices in a random manner, the primary indicator of a network that will have QoS problems is one that has a non-trivial packet loss and/or retransmission rate. Generally, for LAN only operations, there should be virtually no packet loss for existing data traffic. If there are packet loss problems, the physical interconnects should be validated for Cat-5 wiring compliance in terms of signal quality and drop lengths. Additionally, any congestion/broadcast problems should be addressed via better network configuration and segmentation. Elimination of non TCP/IP based traffic on the LAN such as AppleTalk or non TCP/IP based NetBeui traffic should help. Alternatively, such traffic patterns can be isolated to other subnets via the addition of routers or via the deployment of more sophisticated switches that have the ability to segment traffic into distinct VLANs for various ports. However, note that excessive broadcast traffic can be difficult to address via special switch configuration only.

For a detailed understanding of this topic, InSciTek recommends consulting one of the Cisco Network Engineering books. They do an excellent job of exploring the many topics related to proper design and deployment of sophisticated enterprise level networks.

Author:
Jeffrey Szczepanski
Chief Technical Officer
InSciTek Microsystems, Inc.