

Chapter 24

Business Network

After all of the information previously provided, we need to look at what it would take to build a real small business. The system here is just centered on some basic concepts for a startup business, and may not be the most secure, but hopefully will start to tie a multitude of requirements together. We will also add a few more Linux functions that have not been discussed previously.

Concepts Learned in this Chapter

- Many concepts have been provided in all of the previous chapters. Here we will pull them together and build a small business that focuses on using Linux as the primary backbone of the IT operations.

Table of Contents

Business Network.....	1
24.1 Server Requirements.....	3
24.2 Router Requirements.....	4
24.3 Network Setup.....	5
24.4 DMZ.....	6
24.4.1 FTP Server.....	6
24.4.2 HTTP Server.....	6
24.4.3 Mail Server.....	6
24.4.4 DNS Server.....	7
24.5 Local Server Setup.....	9
24.5.1 Samba File Server.....	10
24.5.2 Dynamic Host Configuration.....	12
24.5.3 Database Server.....	12
24.5.4 Data Backup.....	13
24.5.4.1 BK app 1.....	13
24.5.4.2 BK app 2.....	13
24.5.5 IT Management.....	13
24.5.5.1 SNMP Monitoring.....	13
24.6 Staff Network.....	13
24.6.1 Voice over IP PBX Server.....	14
24.6.2 Authentication Server.....	15
24.6.2.1 Open-Radius Authentication Configuration.....	15
24.6.2.2 Open-LDAP Configuration.....	15
24.6.2.3 Certificate Authority.....	15
24.6.2.4 Open S/WAN Configuration.....	15
24.6.3 Wireless Access Units.....	15
24.7 Printer Requirements.....	15
24.8 Router Configuration.....	16
24.9 Environmental Requirements.....	17
24.9.1 Physical Security.....	17
24.9.2 Physical Monitoring.....	17
24.X Commands used in this Chapter.....	18
24.Y Review Questions.....	18

Lets start to put all of the previous chapters together and build a small business network. Just what is required? We will review the requirements and then build a simple network that will provide the services.

One of the most important questions that must be evaluated, but cannot be done in this document, is how many physical servers are required. Than answer depends upon your requirements in what you expect to see in traffic usage. What we will focus on is the server requirements, not the number of physical hosts required to perform the function. At the same time, the diagrams that are shown will depict each server as a separate host – that is for illustration only.

For our example business, we will call our company **NetBusiness.com**. We will use this as our domain name in setting up various configuration files.

24.1 Server Requirements

For a start, lets go back to Chapter 10 and review what servers may be required.

NFS	Used only if directory sharing is required between two or more Unix / Linux hosts. As a general rule, this should not be required. Also remember, NFS can be a security risk.
Samba	Used to set up a shared directory / service between Unix / Linux and Microsoft hosts. It is a good idea to have a host set up to support this functionality if required.
Telnet	For security purposes, this service should always be disabled. The alternative to accessing the servers for configuration from a remote location is to use SSH. By default, Red Hat / Fedora Core has this enabled. You may wish to add additional security by limiting who has access.
FTP	This is an excellent server to support if the business provides downloadable files or software. It is important to insure that the server is maintained in a secure mode to prevent users from logging on and gaining access to inappropriate directories.
TFTP	Unless one is running a thin client (network bootable Linux hosts), this is probably not required.
HTTP	Business is required to be on the Internet today if one is to survive. This is an absolute necessity. Additional features should be investigated to develop enhanced features and additional security.
DNS	If a web and mail server is to be implemented, then this is an absolute necessity. Remember that it must be set up with an off-site redundant system.

DHCP	To minimize the administration of the workstations, it will be a good idea to set up this service.
Mail	As a business, email is an absolute necessity. Traffic on this host may be significant and security is very important. Also remember that email must be monitored for spam and viruses.
Database	An SQL database is very important to a business. Simple flat databases may be used for day-to-day processes, but a full relational database manager is absolutely required. A business web page will also integrate with the SQL database for tracking orders.
Authentication	If an internal wireless network is desired, then for security purposes, authentication is an absolute requirement.
Backup	Data must be protected – a backup server is required to maintain the business' information.
VoIP Phone PBX	In order to optimize the business costs, one can look into using a Voice over IP PBX. This will provide the users a fully functional PBX along with a very low cost.

Each server is to be configured to support SSH access with a passphrase and limited access to only the designated staff.

24.2 Router Requirements

Our first router requirement is for Internet access. This router will provide three functions:

- A. Internet access using a public address.
- B. Local network interface for the De-Militarized Zone (DMZ) for all servers that will be seen from the Internet. These servers will include:
 - 1. FTP
 - 2. HTTP
 - 3. DNS
 - 4. Mail
- C. Local network for the base server requirements that will be for internal usage. This will make up the remainder of the servers not installed in the DMZ.
- D. Local network for the IT requirements. This is presented here as a separate network for security purposes, but may be merged with another network if desired.
- E. Local network for the workstations. This may be actually made up of several different networks if desired for security purposes

For our simple network, we will assume that the business is just starting out and the requirements are for three local networks: DMZ, Server / IT, and workstations. From this, we will have the following network diagram.

The IT department has been combined with the local network server network. This allows for extra security when configuring the servers and additional security to prevent the Internet user from gaining access to the IT department systems.

The DMZ is maintained as a separate network in order to insure security. Network Address Translation is used to port the incoming services to the private network addressing, thus a public address will not be required for each server.

The internal servers and workstations are set up on three separate private address networks in order to provide security isolation. The business servers will be accessible to the work staff, but will remain isolated for security.

A router may be configured from a Linux system, or a commercial router may be utilized. In either case, the configuration of routing tables, Network Address Translation (Masquerading), and Firewall attributes utilizing either Access Lists or IP Tables will be a requirement. Either of these will require an expert for configuration. We will leave the configuration of the router to last.

For documentation purposes, we will assume that the domain IP address will be 200.200.200.16/28, with the router IP address of 200.200.200.18/28; the ISP IP address will be 200.200.200.17/28.

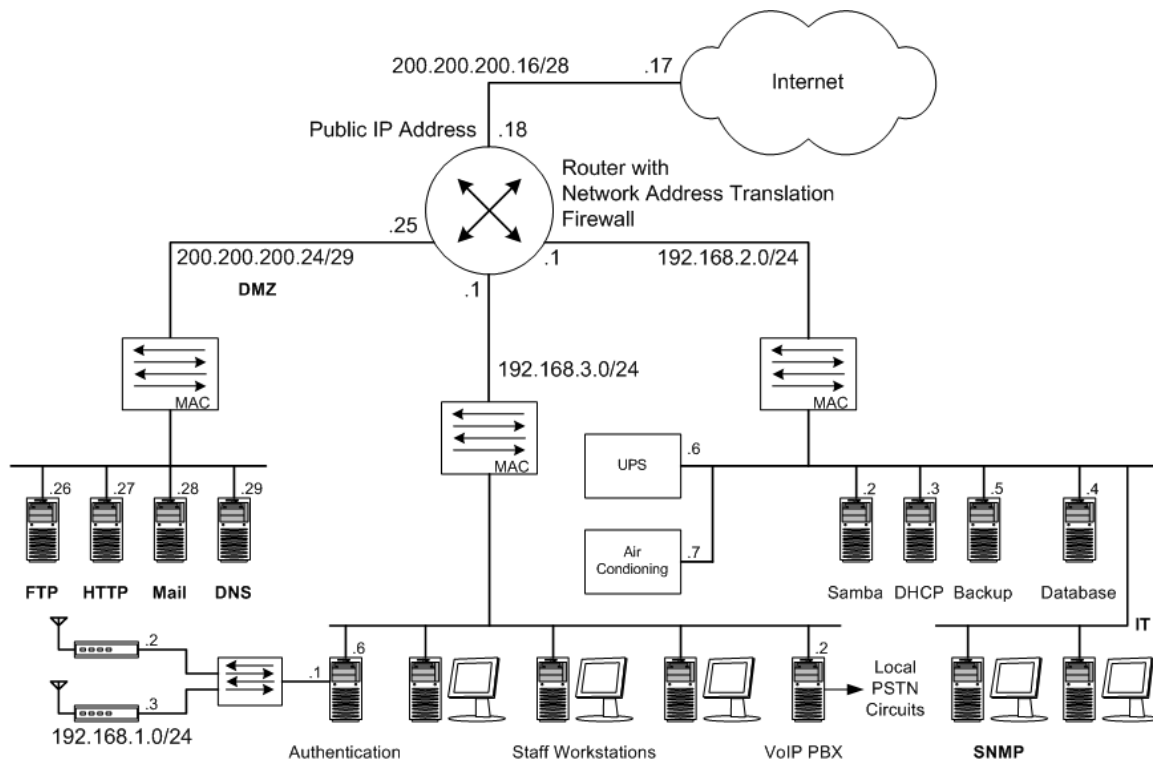


Figure 23-1: Basic Business Network

24.3 Network Setup

The requirement here is to set up the three basic networks on our network. For simple purposes, we will set up each network as a Class 3 network, although Subnetting may be utilized. The DMZ is a subset of the public address range, and it therefore utilizes Subnetting.

Each local network is presented with appropriate details for the addressing and configuration requirements specified as necessary. Configuration requirements are specified, but the activation and starting of the server are not specified, but must be enabled as appropriate.

24.4 DMZ

Our DMZ network will consist of the four server functions. For our discussion, we will set up four separate hosts, although it is not necessary. We will set the following addresses:

Internet Network Address:	200.200.200.16/28
Router Network Address:	200.200.200.18/28
ISP Network Address:	200.200.200.17/28
DNZ Network Address:	200.200.200.24/29
DMZ Ethernet Address:	200.200.200.25/29
FTP Server:	200.200.200.26/29
HTTP Server:	200.200.200.27/29
Mail Server:	200.200.200.28/29
DNS Server:	200.200.200.29/29
DMZ Broadcast Address:	200.200.200.31/29
Internet Broadcast Address:	200.200.200.31/28

24.4.1 FTP Server

The FTP server will be set up in a generic format, thus no special configuration will be required. The business files that are to be made available to the public will be located in the **/var/ftp** directory, and will not allow any uploading of files. If individual users are to be allowed to upload, then they will have their own home directories to work within.

This server will be named **pubdocs**; the Fully Qualified Host Name is therefore (FQHN) **pubdocs.netbusiness.com**.

24.4.2 HTTP Server

The HTTP server will also be set up in a generic format. The public will require general access, and the public will access the **index.html** file from the **/var/www/html** directory.

This server will be named **webdocs**; the FQHN is therefore **webdocs.netbusiness.com**.

We will add more to this later for additional creativity.

24.4.3 Mail Server

The mail server will require configuration for proper operation. In our business, we have decided to implement the MTA application of **postfix**. Postfix is used because it is much simpler to implement and will provide all of the services that we need. The basic configuration file is located in the **/etc/postfix** directory, local mail is maintained in the **/var/spool/mail** directory, and the outgoing mail is maintained in the **/var/spool/mqueue** directory.

This server will be named **post**; the FQHN is therefore **post.netbusiness.com**.

24.4.4 DNS Server

The DNS server will require extensive configuration in order to support the business. We will also need to set up a remote slave DNS server in order to insure redundancy of the business. The basic configuration is maintained in the **/etc/named.conf** file, and the basic domain configuration files are located in the **/var/named/chroot/var/named** directory. Remember, a real business will have different addresses, and will require address consolidation for servers that are combined into one host.

The DNS server is named **netbus**, the FQHN is therefore **netbus.netbusiness.com**.

Configuration of the files will include:

/etc/named.conf – Master Server

```
options {
    directory "/var/named";
};
controls {
    inet 127.0.0.1 allow {localhost;} keys {rndckey;};
};

# IN Domain Forward File
zone "netbusiness.com" {
    type master;
    file "netbusiness.com.zone" ;
};

# Domain Reverse File
zone "200.200.200.in-addr.arpa" {
    type master;
    file "200.200.200.in-addr.arpa.zone" ;
};

# Local Forward File
zone "localhost" {
    type master;
    file "localhost.zone" ;
};

# Local Reverse File
zone "0.0.127.in-addr.arpa.zone" ;
    type master;
    file "0.0.127.in-addr.arpa.zone" ;
};

# Cache File
zone "." {
    type hint;
```

file “named.ca”

```
/var/named/chroot/var/named/netbusiness.com.zone
```

\$TTL 86400

@ IN SOA netbus.netbusiness.com. admin.netbusiness.com.

(

```
2006022400 ; Serial
7200 ; Refresh
3600 ; Retry
43200 ; Expire
86400 ; Minimum
```

)

	IN	NS	netbus.netbusiness.com.
	IN	MX 0	post.netbusiness.com.
netbus		IN A	200.200.200.29
post	IN	A	200.200.200.28
webdocs	IN	A	200.200.200.27
pubdocs	IN	A	200.200.200.26
ns	IN	CNAME	netbus.netbusiness.com.
mail	IN	CNAME	post.netbusiness.com.
mx	IN	CNAME	post.netbusiness.com.
www	IN	CNAME	webdocs.netbusiness.com.
ftp	IN	CNAME	pubdocs.netbusiness.com.

```
/var/named/chroot/var/named/200.200.200.in-addr.arpa.zone
```

\$TTL 86400

@ IN SOA netbus.netbusiness.com. admin.netbusiness.com.

(

```
2006022400 ; Serial
7200 ; Refresh
3600 ; Retry
43200 ; Expire
86400 ; Minimum
```

)

	IN	NS	netbus.netbusiness.com.
29	IN	PTR	netbus.netbusiness.com.
28	IN	PTR	post.netbusiness.com.
27	IN	PTR	webdocs.netbusiness.com.
26	IN	PTR	pubdocs.netbusiness.com.

```
/var/named/chroot/var/named/localhost.zone
```

\$TTL 86400


```

@      IN      SOA  netbus.netbusiness.com.  admin.netbusiness.com.
(
        2006022400 ;      Serial
        7200      ;      Refresh
        3600      ;      Retry
        43200     ;      Expire
        86400     ;      Minimum
)

        IN      NS      netbus.netbusiness.com.
        IN      A        127.0.0.1

```

/var/named/chroot/var/named/0.0.127.in-addr.arp.zone

\$TTL 86400

```

@      IN      SOA  netbus.netbusiness.com.  admin.netbusiness.com.
(
        2006022400 ;      Serial
        7200      ;      Refresh
        3600      ;      Retry
        43200     ;      Expire
        86400     ;      Minimum
)

        IN      NS      netbusiness.com.
1      IN      PTR      netbusiness.com.

```

/var/named/chroot/var/named/named.ca

This file is not modified.

24.5 Local Server Setup

We now need to configure the local servers. These are located on the 192.168.2.0 network and are available from by the staff, but are secure and inaccessible from the external Internet. The servers on this network consist of:

Samba	This is the general file server for the staff. Files may be easily shared through this server.
DHCP	Staff computers will be configured with this server for the various required addresses.
Database	The web server (webdocs) and staff will have access to this server for creating sales, leads, and general operation for the business.
Backup	All data must be backed up for the security of the business. This server will provide appropriate interfaces to various backup devices, which may include hard drive, CD burner, DVD burner, and tape drives.

The following addresses will be assigned to the server network:

Server Network Addresses: 192.168.2.0/24
 Router Ethernet Address: 192.168.2.1/24
 Samba Server: 192.168.2.2/24
 DHCP Server: 192.168.2.3/24
 Database Server: 192.168.2.4/24
 Backup Server: 192.168.2.5/24
 Broadcast Address: 192.168.2.255

24.5.1 Samba File Server

To promote the general storage of files to the staff, a Samba server is set up to allow a shared storage area. Here we will provide several examples, but additional directories may be configured in like manner if specific staff access is required.

The following directory structure is created to support the various departments:

```

/share/
/share/marketing
/share/sales
/share/hr
/share/executive
/share/development
/share/manufacturing
  
```

The directories below /share are set up with the following attributes:

<u>Directory</u>	<u>Permissions</u>	<u>Group</u>
marketing	rwxrws	marketing
sales	rwxrws	sales
hr	rwxrws	hr
executive	rwxrws	executive
development	rwxrws	development
manufacturing	rwxrws	manufacturing

Appropriate individuals are added to the specified groups for access to the respective directories.

We now need to edit the **/etc/samba/smb.conf** file. The first modification that we wish to make is to the **Global** section; here we change only the workgroup and netbios name for the server. Lets set them to:

```

netbios name = netbussvr
workgroup = businessvr
  
```

All other settings in the global section may be left with no alteration.

In the **Private** section, we will add sections for each directory, but do not need to make any other changes. For our example, these additions include:

```

[Marketing]
comment = Marketing Directory
path = /share/marketing
  
```

```
writeable = yes  
browseable = yes  
valid users = @marketing  
locking = yes  
create mode = 0770  
directory mode = 0770
```

[Sales]

```
comment = Sales Directory  
path = /share/sales  
writeable = yes  
browseable = yes  
valid users = @sales  
locking = yes  
create mode = 0770  
directory mode = 0770
```

[HR]

```
comment = Human Relations Directory  
path = /share/hr  
writeable = yes  
browseable = yes  
valid users = @hr  
locking = yes  
create mode = 0770  
directory mode = 0770
```

[Executive]

```
comment = Executive Directory  
path = /share/executive  
writeable = yes  
browseable = yes  
valid users = @executive  
locking = yes  
create mode = 0770  
directory mode = 0770
```

[Development]

```
comment = Development Directory  
path = /share/development  
writeable = yes  
browseable = yes  
valid users = @development  
locking = yes  
create mode = 0770  
directory mode = 0770
```

```
[Manufacturing]
comment = Manufacturing Directory
path = /share/manufacturing
writeable = yes
browseable = yes
valid users = @manufacturing
locking = yes
create mode = 0770
directory mode = 0770
```

Now the groups need to be created and the appropriate users added to them. Before adding a user to the smbpasswd file, make sure the user is added as a normal user to the normal passwd file. The **/etc/samba/smbpasswd** file also needs to be created.

24.5.2 Dynamic Host Configuration

All of the staff will be configured for **dhcp**, thereby reducing the amount of work required by the administrator. The **/etc/dhcpd.conf** file must be created with information like the following:

```
/etc/dhcpd.conf
default-lease-time      3600;
max-lease-time          43200;

option subnet-mask      255.255.255.0;
option broadcast-address 192.168.3.255;
option routers          192.168.3.1;
option domain-name "netbusiness.com";
ddns-update-style       ad-hoc;

subnet 192.168.3.0 netmask 255.255.255.0 {
    range 192.168.3.24 192.168.3.250;
}
```

Remember to also create the **/etc/dhcpd.leases** file.

24.5.3 Database Server

In this business, we will utilize the MySQL database. This is a good choice as not only does it support all SQL functions that will be required, it also integrates well into the Linux – Apache – MySQL – Perl / Python / PHP applications. LAMP is a development concept that integrates the process to produce very fast web pages and support.

MySQL is a straightforward setup. Performing the installation and activation, and it is operational. The only requirement is to set up the administrator and appropriate users with designated rights.

Setting up of various applications and databases is not reviewed here, as it is a business specific topic.

24.5.4 Data Backup

The data maintained on the various servers must be protected on a periodic basis. Several applications are available within Linux, both commercial and free / open-source applications, to allow one to provide the required protection.

24.5.4.1 BK app 1

24.5.4.2 BK app 2

24.5.5 IT Management

IT must maintain access to all equipment, including routers, servers, and hosts. For security purposes, it is located on the local server network, but may be on its own separate network if desired. Within the router, access from the network is provided to all other devices.

24.5.5.1 SNMP Monitoring

In order to allow the ease of monitoring the network operation, the IT department is equipped with an SNMP client agent. This unit will query the router, MAC switches, servers, UPS, and Air Conditioning equipment for operational status. The GUI display will be set up to show the operational status of each device, and allow the display of the operational status of each interface, including traffic analysis.

Each device that is to be monitored will be configured with the community name of **netbus**. Although net-snmp at this time does not support SNMP version 3, the network should be set to function at a level of SNMP version 2, with upgrading when available.

24.6 Staff Network

The staff network consists of various departmental functions to support the executive, marketing, human resources, sales, development, and manufacturing. Additionally, the network will support the VoIP switch and wireless access Authentication server. These groups may be grouped together as Virtual LANs or just merged together. The initial configuration of the network will require several static address assignments for the router Ethernet interface, various Jet-Direct Printer assignments, Authentication server, and the Voice over IP PBX server. All workstation hosts are configured to obtain their network parameters from the DHCP server, where the router is configured to relay the DHCP requests to the DHCP server. In our configuration, we show two Wireless Access units, but more may be necessary for complete coverage to the business area. For static requirements, the required settings would be:

VoIP Switch: 192.168.3.2/24

Authentication Server – Staff: 192.168.3.6/24
 Authentication Server – Wireless: 192.168.1.1/24
 Wireless Access Unit #1: 192.168.1.2/24
 Wireless Access Unit #2: 192.168.1.3/24

VoIP Server Local voice communications is supported with a Voice over IP PBX. This provides interconnection to the local PSTN for local and long distance calls. If it is known that another business also supports a VoIP PBX, these may be routed via the Internet.
Authentication If a wireless network is installed, then an authentication server is required to insure that the users are authorized. Additionally, this server will include a Virtual Private Network (VPN) to insure that all transmitted information across the airwaves is secure.

24.6.1 Voice over IP PBX Server

In order to provide a cost effective phone system, a Voice over IP PBX is recommended to provide the various services. The Asterisk application provides this functionality in a superb manner. Features that are available by using Asterisk include:

- A. Analog and Channelized digital call service to the Public Switched Telephone Network (PSTN)
- B. IP call service to other VoIP PBXs
- C. Automatic long distance route selection
- D. Long distance call service via a VoIP service provider
- E. Call Transfer
- F. Call Forwarding
 - 1. No Answer
 - 2. Busy
- G. Abbreviated Dialing
- H. Speed Dialing
- I. Music on Hold
- J. Voicemail

The system will require the setting up of several configuration files. In this example, the call pattern will be set up for 4 digit extensions and the following properties:

PSTN Access: 9 Access
 Long Distance Access: 1+
 Local Extensions: 4XXX

On dialing the digit “9” for an external connection, the PBX issues a second dial tone, whereupon the system monitors for the first digit being a “1”. If it is a “1”, the PBX will analyze the dialed number and select the optimum route, to the PSTN or to a VoIP service provider if available.

The static IP address of the VoIP PBX will be set to 192.168.3.2/24.

The files requiring configuration are:

24.6.2 Authentication Server

Authentication of wireless users will be set up as a two-part process. The first will be to authenticate the user through the use of the two server functions, Open-Radius and Open-LDAP. These will insure that the user is properly authorized to access the network.

As a second requirement, it is necessary to insure that all transmissions are secure from any other party being able to monitor the content. To insure this the transmissions must be encrypted. Thus, each wireless device will be configured to support Virtual Private Network (VPN) between itself and the Authentication Server, which will also be configured for VPN. The software to be utilized to support the VPN will be Open S/WAN.

24.6.2.1 Open-Radius Authentication Configuration

24.6.2.2 Open-LDAP Configuration

24.6.2.3 Certificate Authority

24.6.2.4 Open S/WAN Configuration

Open-SWAN provides the configuration of a user to support VPN. IPsec is supported to between various systems. Connection may be made between either a server-to-server connection or host-to-server connection.

24.6.3 Wireless Access Units

The wireless access units, other than being configured for an IP address to allow configuration access, no other special configuration will be made. Because the of the Authentication server being configured for limiting access and the use of VPN, unauthorized users will be able to connect to the access unit, but will not be able to go beyond the Authentication server.

24.7 Printer Requirements

The printer requirements in a business may be served in one of three ways:

- A. Windows Print Sharing

- B. Unix / Linux Print Sharing using Samba
- C. Jet-Direct Printers

If one allows diverse business requirements, then the best option is to obtain a printer that supports Jet-Direct, or a direct Ethernet connection. Users may then send documents to the static IP address assigned printer. Other than configuration of the host workstations for accessing the printer via an IP address, no other requirements exist.

24.8 Router Configuration

This is a very limited presentation of what is required to set up Linux as a router. This process is quite complex and errors may easily be made, thus leaving the business either inoperative or open to security hacks.

This example is not exhaustive and requires considerable additional work, but is intended to show the concept of what is required rather than be a correct configuration.

For our example business, the router will require four interfaces, three Ethernet for local connection and one serial for Internet connection via the ISP. If the business elects to be served by either DSL or Internet Cable service, then the forth interface would also be Ethernet. The address assignment for the interfaces is:

ISP Internet interface:	200.200.200.18/28
DMZ Network interface:	200.200.200.25/29
Internal Server Network:	192.168.2.1/24
Staff Network:	192.168.3.1/24

The router must be set up with various restrictions to allow traffic to flow as necessary. These include:

Internet Interface:	
DMZ Network:	Connection to DMZ Network allowing only appropriate port access for the specified servers (DNS:53, HTTP:80, Mail:25, FTP:20/21, SSH:22). All other service originations access should be blocked.
Local Server Network:	Access to the Local Server Network is denied.
Staff Network:	Access to the Staff Network is directly blocked, but may respond to NAT response queries from the Staff Network.
DMZ Interface:	
Internet Interface:	No origination requests are required to the Internet. Responses to queries are allowed.
Local Server Network:	The only access to the Local Server Network will be to support requests for MySQL service by the web server.
Staff Network:	No origination requests are required to the Staff Network.
Local Server Interface:	

Internet Interface:	No origination requests are required to the Internet. The Internet does not require access to this network.
DMZ Network:	No origination requests are required to the DMZ Network. Responses to queries from the web server are permitted.
Staff Network:	No origination requests are required to the Staff Network. Responses to all requests are required.
Staff Network: Internet Interface:	Many requests to the Internet will be made; requests are Network Address Translated to the public IP address for security purposes. No direct access is to be allowed.
DMZ Network:	Queries to the various servers is required. Port access should be limited to previously specified ports.
Local Server Network:	Queries to the various servers is required. Port access should be limited to previously specified ports.

24.9 Environmental Requirements

Everything up to this point has been directed to the configuration of the network equipment. There are several other security and operational requirements, that of physical security and the operational plant.

24.9.1 Physical Security

The physical security of the router and servers is also very important to the business. This equipment should be maintained in a locked room with access only to the IT staff. If additional security is desired, the room may also be secured with an alarm system that is designed to allow only authorized code access. This unit may also provide a log of who has entered and when if the appropriate unit has been purchased.

24.9.2 Physical Monitoring

Two requirements may exist that may also be monitored, an Uninterruptible Power System (UPS) and the facility air conditioning.

To insure that all of the routers are maintained in an operational state, an Uninterruptible Power Supply should support the router and all servers. This unit should have an Ethernet interface that would allow the unit to be monitored by the SNMP system. Thus the status of the unit may be continually monitored as to its performance.

If available, the air conditioning system may also be monitored by the SNMP system to insure that it is operating properly. This would allow the unit to also be maintained by the

24.X Commands used in this Chapter

24.Y Review Questions

Chapter Index

A		IT Management	13
Application		L	
Asterisk VoIP Switch	14	Local Server Setup	9
Open S/WAN Server	15	Backup	9
Open-LDAP Server	15	Database	9
Open-Radius Server	15	DHCP	9
Asterisk		Samba	9
PBX Features	14	localhost.zone File	8
Asterisk VoIP Switch	14	M	
Authentication		Masquerading	5
Open S/WAN Server	15	N	
Open-LDAP Server	15	named.ca File	9
Open-Radius Server	15	named.conf File	7
Wireless Access Units	15	NAT	5
B		Network Address Translation	5
Business Network Setup	5	O	
Business Printer Requirements	15	Open S/WAN Server	15
Business Router Configuration	16	Open-LDAP Server	15
Business Router Requirements	4	Open-Radius Server	15
Business Server Requirements	3	P	
D		PBX Features	14
DeMilitarized Zone	4	Physical Monitoring	17
DMZ	4	Physical Security	17
DNS Server	7	R	
FTP Server	6	Reverse Domain Zone File	8
HTTP Server	6	Reverse Localhost Zone File	9
Mail Server	6	S	
DMZ Network	6	Server	
DNS Forward Zone File	8	Authentication	4
E		Backup	4
Environment Requirements		Database	4
Physical Monitoring	17	DHCP	4
Physical Security	17	DNS	3
Environmental Requirements	17	FTP	3
F		HTTP	3
File		Mail	4
Reverse Localhost Zone	9	NFS	3
/etc/named.conf	7	Samba	3
/var/named/Domain Forward Zone	8	Telnet	3
/var/named/localhost.zone	8	TFTP	3
/var/named/named.ca	9	VoIP Phone PBX	4
/var/named/Reverse Domain Zone	8	Server Requirements	3
FQHN	7	SNMP Monitoring	13
Fully Qualified Host Name	7	Staff Network	13
I		Authentication Server	14

VoIP Switch	13	UPS	17
Wireless Access Unit	14	W	
U		Wireless Access Units	15
Uninterruptible Power Supply	17		