

Open Source Communication Options

By
Practical Support, Ltd.
2012

About Practical Support, Ltd.

- Practical Support is a local business and since 1999 has been providing solutions for secure data communication and voice over internet protocols (VoIP). Our goal is to provide the most practical cost effective solution that will meet the needs of our customer.
- Our projects have ranged in size from restructuring and upgrading networks with 2000 plus network devices to small offices supporting only 2 people.
- If your business has one location or multiple locations we can develop a solution that will meet your data communication requirements.

Presenter

- Eugene Spiker
- President of Practical Support, Ltd.
- 45 Years in the communications industry
- Designed and Implemented many communication networks using a multitude of technologies, protocols, and equipment.

Basic Communication Components

- There are two basic components to communications:
 - The creation of the information to be communicated
 - The transmission of that information.
- The focus of Practical Support is the transmission of information and the means to do it securely and cost effectively.

Information Transmission

- The transmission of this information requires the following basic elements:
 - Connection to and communication with the Internet (Router)
 - Securing the connection (Firewall)
 - Securing the data communicated (Security Applications)
 - Transmission of voice communications over the Internet (VoIP)
 - Monitoring of transmission status (Bandwidth reports, device monitoring)
- Each company has different types of requirements and the level of support required for each of the above basic elements and Practical Support can provide solutions ranging from consulting and support for a specific element to turnkey solutions for self-installation to completely managed systems.

Goal of Presentation

- Provide an overview of basic network designs requirements
- Provide an overview of the some of the optional Open Source products available
- Provide information on how Practical Support can assist with your efforts to build a secure, reliable, cost effective communication system for your company.

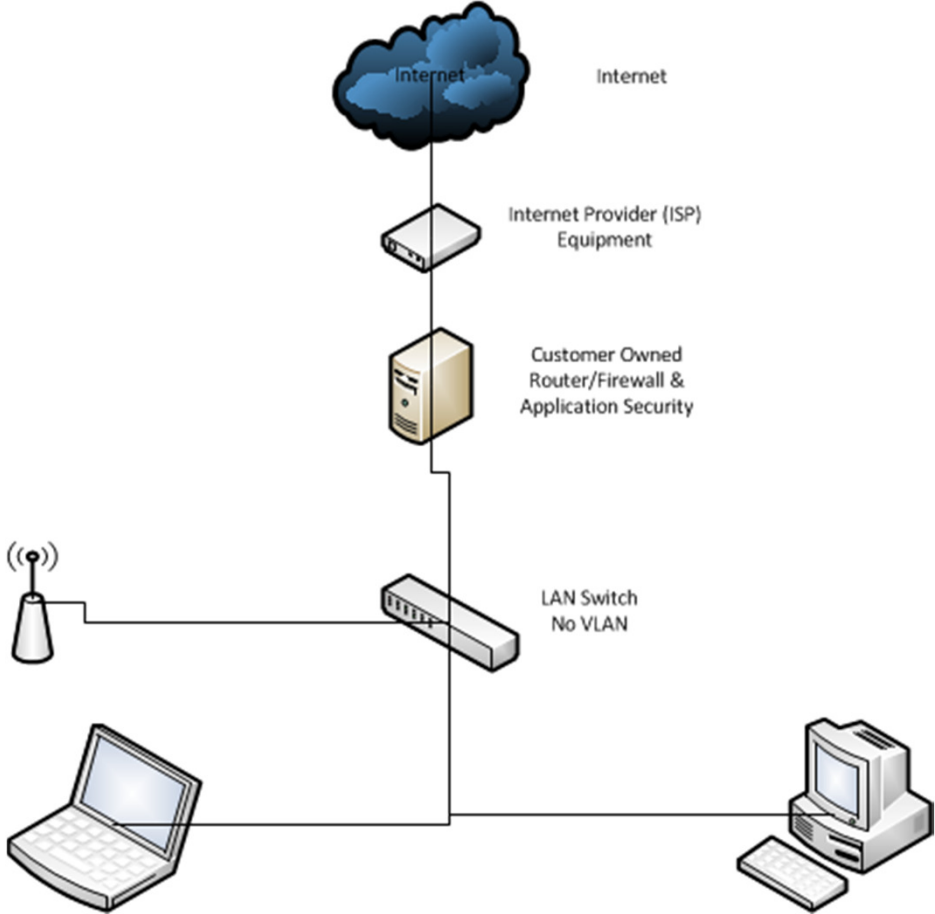
We will Discuss

- Network Designs
 - Basic Single office Network
 - Multiple Office with Inter-Office communications
 - Description of over the counter commercial routers
 - When to separate functions
 - Description of what a router does
 - Description of what a firewall does
 - Description of Security applications
 - Description of Verification applications
 - Description of VoIP
- Open Source Solutions
 - Routers
 - Firewalls
 - Security Applications
 - Monitoring Applications
 - VoIP
- General Recommendations
 - When to use something other than over the counter routers

Basic Secure Single Office Network

- Characteristics
 - One location
 - Single connection to the Internet
 - All network devices wired to a single hub location
 - A single wireless access point located at hub location
 - No Internet servers on site
 - Bandwidth monitoring required
 - Internet usage monitoring required
 - WEB filtering required
 - All SPAM/Virus checking done centrally and on individual PC's
 - Only employees use the network

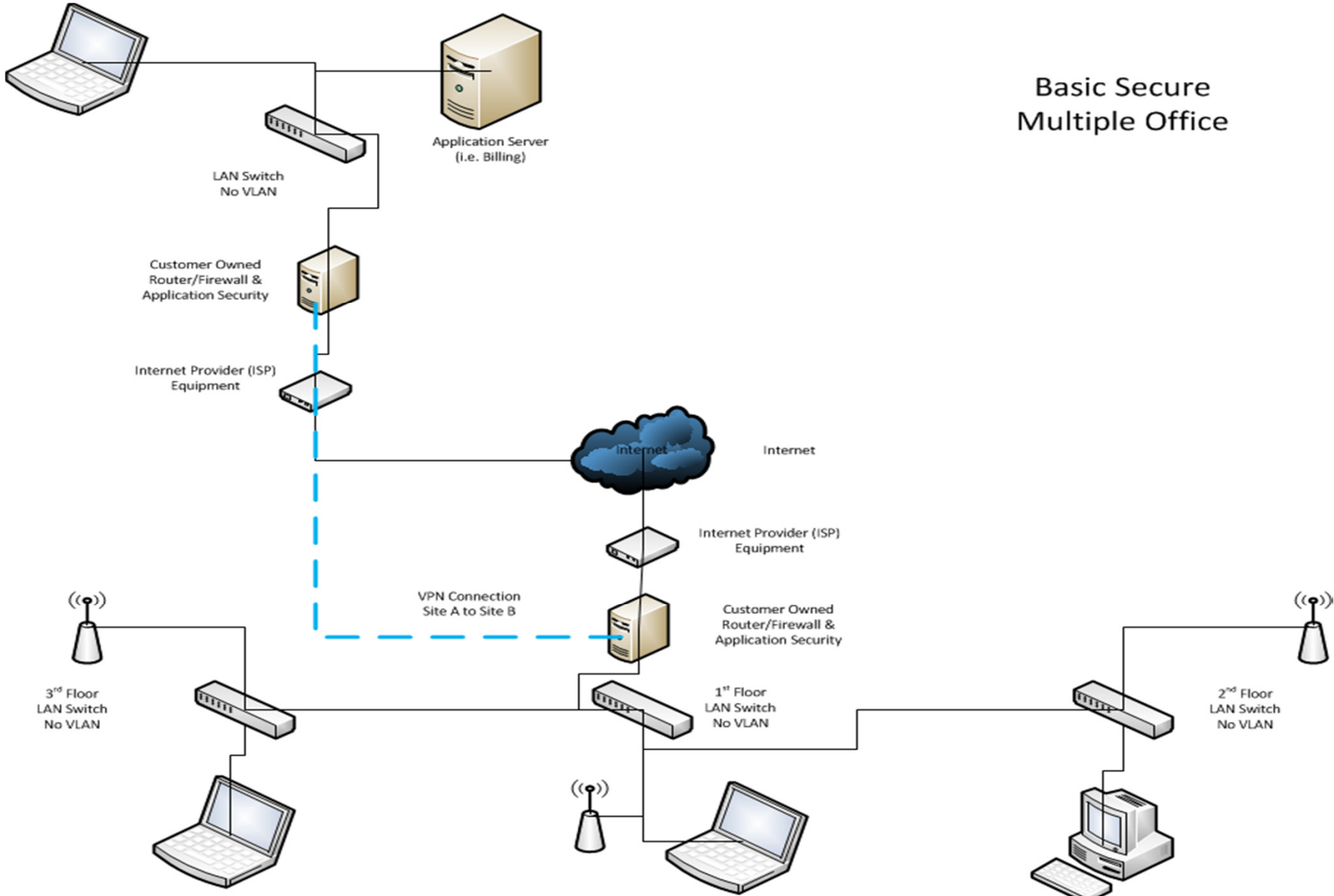
Basic Secure Single Office Network



Basic Secure Multiple Office

- Characteristics
 - Multiple locations
 - Single connection to the Internet for each location
 - Secure communications required between interoffice devices
 - Main communication devices located at hub location for each site
 - PC's and other network devices connected to multiple LAN switches
 - Multiple Wireless Access points required at some offices
 - Bandwidth Reports required
 - WEB usage reports required
 - WEB filtering required
 - SPAM/Virus checking done centrally and on each PC
 - No Internet Servers at any location
 - Only employees use the network

Basic Secure Multiple Office



Over the Counter Retail Routers

- Combines the following into one unit:
 - Basic NAT/Router functions
 - Basic Firewall
 - 5 Port LAN Switch
 - Wireless Access Point
- Advantages
 - Low Cost
 - Simple setup
 - All in one unit
- Disadvantages
 - Designed to support 10 or fewer network devices
 - No usage reports
 - No bandwidth reports
 - Limited or no expansion capabilities
 - Primary security provided by Network Address Translation (NAT)
 - NAT is not available in the IPv6 world
 - Limited software upgrades
 - No site to site secure communications

A Word on IPv6

- IPv6 is the new Internet address method and will eventually replace IPv4
- Replacement will take many years
- IPv6 is being implemented because we have run out of IPv4 addresses
- Current IPv4 addressing has two basic types of addresses Public and Private.
 - Public addresses are known to the world
 - Private addresses are only used within a company and can not be accessed via the Internet
- Most small and medium businesses use Network Address Translation (NAT) to use a single public IP address for all of their Internet transactions
 - All inside addresses look like the same out side public address via NAT
- NAT is not available in IPv6. All addresses are **public**.
- In the IPv6 world the use of a properly configured firewall is going to become extremely important. If not configured properly individual PC's will be open to the public.
- Most small to medium size businesses will not have to worry about IPv6 for a few years.
- If you are connecting to another larger business that has decided to use only IPv6 then you will have to implement IPv6 also. The two numbering systems do not translate.

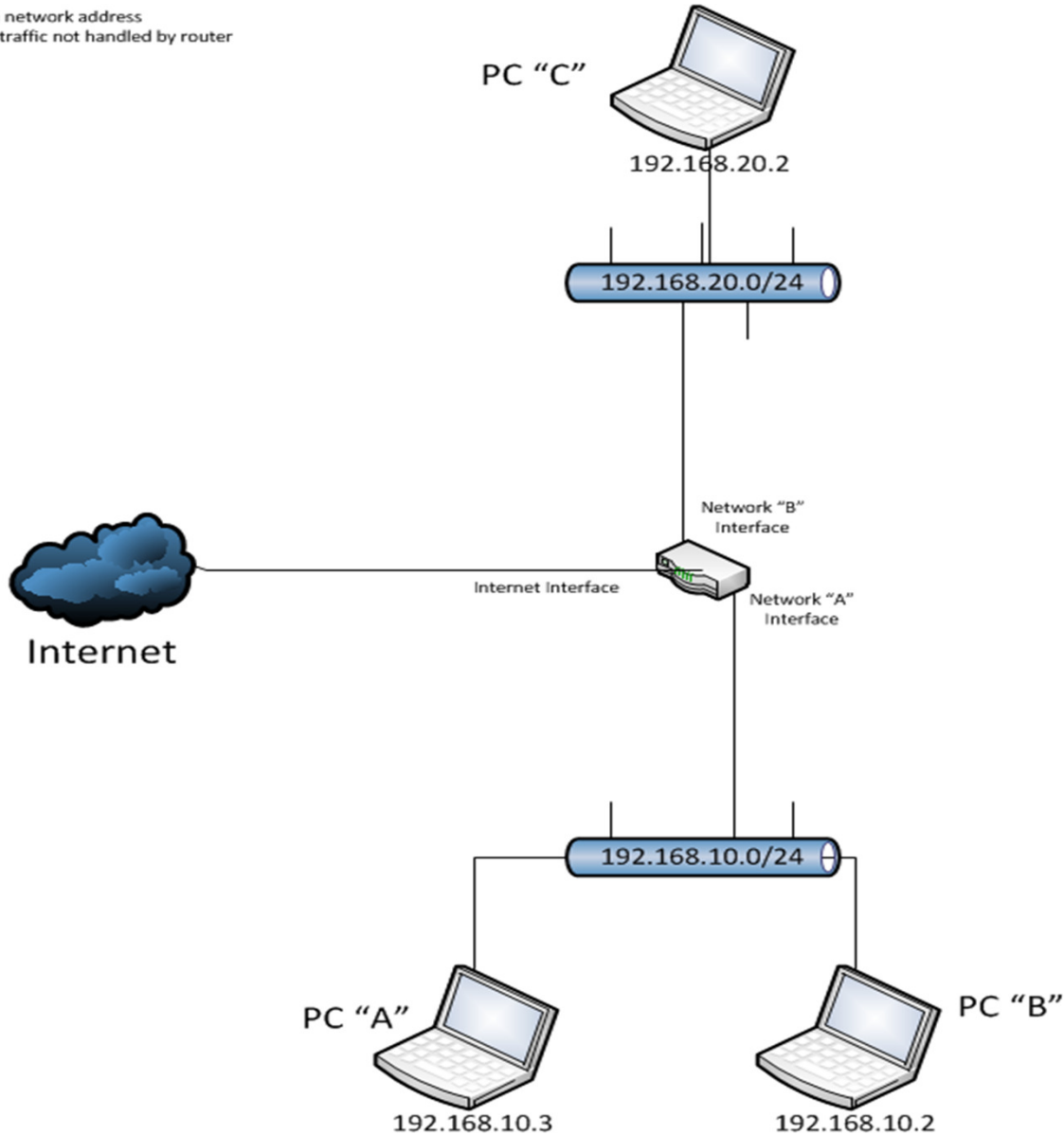
When to separate functions

- When you expand to multiple locations requiring secure site to site communications
- When your user count surpasses the capacity of the retail router
- When you need to use large or multiple LAN switches
- When you need multiple wireless access points to provide coverage to the office
- When you need to meet industry specific security and reporting requirements (HIPPA, PCI, etc.)
- When you need to implement human resource requirements for WEB filtering and usage reporting
- When you want to add an additional level of security by use of WEB and Mail proxy servers
- When you implement onsite Internet Servers
- If you need to implement Internet addressing version 6 (IPv6)

Description of what a router does

- Definition - A network device that forwards packets from one network to another. Based on internal routing tables, routers read each incoming packet and decide how to forward it. The destination address in the packets determines which line (interface) outgoing packets are directed to. In large-scale enterprise routers, the current traffic load, congestion, line costs and other factors determine which line to forward to.
- Simple to think of it as routing local and long distance calls. Based on the IP address (telephone number) the router sends the call to the next town (network) or keeps the call local.
- The next slide gives some simple examples.

Rules:
Routing based on network address
All local network traffic not handled by router



Example 1 – PC "C" sends traffic to device not in 192.168.20.x network range

1. Router looks at IP address of device to be connected.
2. Identifies that it is not part of 192.168.20.x range
3. Identifies it is not part of 192.168.10.x range
- 4 Sends it out Internet interface to next router

Example 2 – PC "C" sends traffic to PC "A" in 192.168.10.x network range

1. Router looks at IP address of device to be connected.
2. Identifies that it is not part of 192.168.20.x range
3. Identifies it is part of 192.168.10.x range
- 4 Sends it out network "A" interface to device

Example 1 – PC "A" sends traffic to PC "B" in same 192.168.10.x network range

1. Router looks at IP address of device to be connected.
2. Identifies that it is part of the same 192.168.10.x range
3. Does nothing

What is a firewall?

- Definition - A firewall is a set of related programs with defined rules, located at the entrance to a network, that protects the resources of one network from users of other networks based on a defined security policy.
- In other terms the firewall is an automated guard at the entrance to your local network. The guard has a set of rules that says who may enter and even what they can carry (no file transfers). The guard can also be positioned between internal networks of users so that the accounting department is off limits to users in the research department. All based on rules in the Firewall configuration.

Description of Security applications

- Security Applications are enhancements to a firewall. They can be implemented as addon's, separate programs or incorporated into the firewall program itself.
- Examples of Security applications:
 - WEB Proxy Server
 - Mail Proxy Server
 - Virus Checker
 - Spam Checker
 - WEB Filters
 - Intrusion Detection Systems

Monitoring/Logging Applications

- Monitoring/Logging applications provide the ability to identify the current status of network operations, identify trends, and trouble shoot network problems based on current and historical information.
- This information can include:
 - Bandwidth usage
 - User WEB site tracking
 - User bandwidth usage
 - System error logging
 - Tracking of all telephone calls
 - Other data reports based on the systems implemented

Most Common Security Problem

- Improper configuration of wireless networks
- Always at minimum do the following:
 - Do not put your company name in the SSID
 - Secure the wireless signal with a security code
 - Use the most secure code your equipment can use
 - If only WEP is available, consider upgrading your equipment
 - Do not hand out the security code to sales people, neighboring businesses, friends and relatives. Employees only.
- If you need to provide wireless to visitors build a separate network firewalled from the company network

VoIP or IP PBX

- An IP ([Internet Protocol](#)) PBX ([Private branch exchange](#)) is a business telephone system designed to deliver voice or video over a data network and interoperate with the normal Public Switched Telephone Network ([PSTN](#)).
- [VoIP](#) (Voice over Internet Protocol) gateways can be combined with traditional [PBX](#) functionality enabling businesses to use their managed [intranet](#) to help reduce [long distance](#) expenses, enjoy the benefits of a single network for voice and data and advanced [CTI](#) features or be used on a pure IP system which in most cases give greater cost savings, greater mobility, and increased redundancy.
- An IP-PBX can exist as a hardware object, or virtually, as a software system.
- Asterisk is a Open Source IP based PBX system is wide use.
- The original Asterisk application while very a very solid, secure and cost effect program is not all that easy to manage from a user perspective.
- Many front end applications have been developed to assist with the management and implementation of Asterisk.

PBX Features

- Single Phone number for all employees
- Auto Attendant gives the big company feel
- Can provide a unique telephone number to select employees
- Voice Mail for all employees available
- Conferencing
- Remote Voice Mail pickup
- Forwarding of VM messages via Email
- Call Records (from and to) including length of call
- Call redirection for vacation etc.
- Possible to locate extensions in employee homes
- Possible to provide phone software on laptops for remote access employees

Cost Effective IP PBX methods

- Deploy a version of Asterisk that is comfortable to you
- Use quality VoIP telephones
- Use SIP trunks instead of direct analog lines
 - Additional interface cards are required for analog lines
 - Depending on your Internet circuit bandwidth capability you may need to deploy analog lines to maintain voice quality
 - SIP Trunks can cost as low as \$12/month for a single phone number and \$.029 per minute

Open Source

- What is it?
 - In production and development, **open source** is a philosophy, that promotes free redistribution and access to an end product's design and implementation details
- Is there support?
 - Community Support
 - Paid Commercial Support in some cases
- Is it reliable?
 - Open Source Apache WEB servers are used for 63% of all WEB sites and 66% of the top million busiest WEB sites
- Is it secure?
 - Part of Open Source philosophy is that the source code is available for any one to examine.
 - Patches and fixes are found by the community quickly
- What does it cost?
 - Free if Community versions are used
 - Licensed Supported versions are available in some cases providing additional support and features

Open Source Solutions

- Mikrotik (Router/Firewall)
- Endian (Firewall/Router/Security Applications)
- Monowall (Firewall/Router/Security Applications)
- Ntop (Bandwidth Monitoring Application)
- Nagios (Device Monitoring Application)
- PBX in a Flash (VoIP)
- Fonality trixbox (VoIP)
- Others available in each category depending on features required.

General Recommendations

- There are no hard and fast rules that define the specific elements needed to build a secure network.
- The simpler the network the simpler the configuration and the tools required.
- The more complicated the network and the environment the more complicated and costly the network design and tools become.
- If you don't know what you are doing and the information on your network is crucial to your business then at the very least have a security review of your network performed by Practical Support.
- Secure your wireless networks. If you need assistance please contact Practical Support.
- Open Source tools are a good cost effective alternative to build secure communication networks.

Contact Information

- Practical Support, Ltd.
- P.O. Box 628
- Brunswick, OH 44212
- Telephone 216-502-4686
- Email sales@practicalsupport.com
- WEB Site www.practicalsupport.com