Dealership Infrastructure Guidelines

Version 2015

Dealership Infrastructure Guidelines: Version 2015

Editor:
Paco Escobar, STAR

Robin Schaffer, STAR

Contributors:
Bill Fitzpatrick, NADA

Jason Loeffler, Karmak

John Lebel, Karmak

Sarah Condiff, Navistar

Dave Carver, STAR

Bridget Almas, STAR

Richard Malaise, NADA

Paco Escobar, STAR

Corrado Luppi, Asconauto

Table of Contents

List of Figures

PREFACE

I.I. STAR ORGANIZATION

An important goal of the STAR (Standards for Technology in Automotive Retail) infrastructure project is providing recommendations about the business-to-business communication requirements within the up-stream supply chain in the automotive industry. These recommendations are intended to reduce maintenance and integration costs for supporting dealerships. This document identifies common requirements and measures dealers can take to ensure an effective information technology (IT) infrastructure.

The STAR Organization is comprised of several Work Groups (WG) that address specific points of interest to the automotive retail industry. The STAR Data WG is chartered with developing and maintaining the XML Business Object Documents (BODs) and the Data Transfer Specification (DTS) data formats while the Infrastructure WG is chartered with finding common infrastructure and interoperability among STAR members. The Infrastructure WG produces two guidelines:

- The Dealership Infrastructure Guidelines (DIG) (this document) - a publication for dealerships providing a guidebook and deployment handbook for IT infrastructure at the dealership.
- STAR Transport Guidelines - a high level requirements and recommendations document.
    - STAR Web Services Implementation - implementation details for using Web Services specifications
    - STAR ebMS Implementation Guidelines - implementation details for using the ebXML Message Services specification

I.II. SUMMARY OF CHANGES FROM 2015v1.0

The STAR 2015v1.0 has the following changes:

- Changes were made to the following chapters:
    - Cloud Computing and Virtualization: This is a new Chapter

I.III. SCOPE

The continuing growth in the need to deliver data and solutions to dealerships compels automotive manufacturers, herein referred to as OEMs (Original Equipment Manufacturers), to evaluate both the current methods and plans for meeting future requirements. This document identifies the overall direction chosen. It also explains choices available to a dealer to standardize dealership infrastructures and communication solutions.

The OEMs long-term vision is to migrate all applications to a web-based format. These applications are accessible from any authorized Personal Computer (PC) in the dealership, regardless of the application's

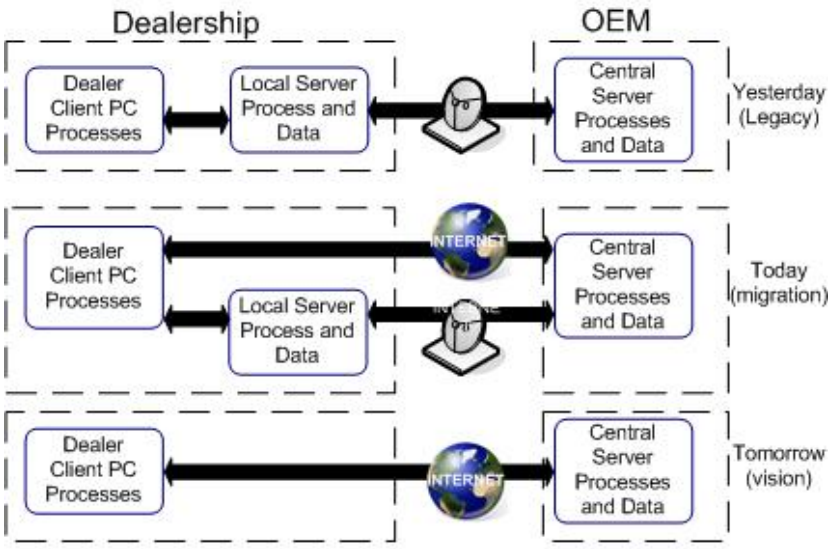
residence. Specific information on legacy systems, migration path, timelines, and other country specific information is found in the attached OEM executive summary and addendum (if applicable).

This document is for network administrators, project leaders, engineers or contractors who are responsible for designing networks and connecting dealerships to OEMs. For the benefit of non-technical readers, the important elements are presented in both an overview and in detailed form.

I.IV. BACKGROUND

Currently some applications run from the OEM's Information Systems servers in the dealerships and some run on central servers accessible through the Internet. It is the vision that all OEM applications will run from central servers located separately from the dealership's site accessible through the Internet using browsers (see Figure 1, “System Migration”). Legacy applications are currently being rewritten to work within the newer environment (see each OEM's addendum for specific information).

Figure 1. System Migration



An external path to the data on the central server is required. Due to the volume of traffic required for dealership applications, the existing link to OEMs using the current satellite technology may not be adequate. Even small dealerships might find the delay of the medium unacceptable. That leads to the need to communicate over a faster and larger medium. The most likely choices include telephone services like a Digital Subscriber Line (DSL) and a T1.

Data circuits using telephone technology have been used for years in situations where capacity or speed is critical or where the number of sites cannot justify broadcast media such as satellite. Many dealerships use data circuits today to link remote sites with a central office or other dealerships. Though very efficient and reliable, some offerings are expensive. This is especially true if separate circuits are required for individual purposes. Therefore, a key to using a data circuit is to leverage the cost by getting as much reuse as possible.

The growth of e-commerce and customers utilizing the Internet to gather and compare information is driving the need for every dealership to use the Internet on a daily basis. Combining the dealers need to

access Internet with the need to exchange data with OEM's is a logical approach to maximize the benefit of the internet.

I.V. OEM VISION

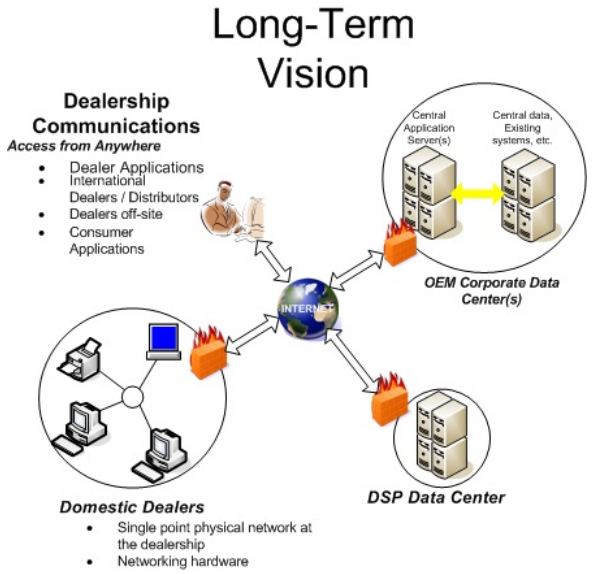
It is the vision of the OEMs that all data communications with the dealerships will be done over the Internet (Figure 2, “OEM Vision”) . This will reduce the reliance on OEM-specific private data networks in the dealerships as the industry moves forward. To realize this vision, the dealerships' infrastructure must be enabled for web applications. PCs connected to a dealership network with access to the Internet will be needed in order to access the applications running on OEMs central servers. This eliminates the need for a private OEM Local Area Network (LAN) in the dealership and thereby reduces support and administration requirements. Serial terminals (green screens) used today for dealership applications and business system workstations will not fill this role. Those terminals can remain in the dealership for use with the business system as long as the Dealership Service Provider (DSP) supports them.

In the briefest terms, the dealership must provide:

- An Ethernet LAN designed and built to computer industry standards.
- Computers powerful enough to run the OEM's applications attached to that network.
- A method of accessing the Internet built into the LAN.

Examination of individual dealerships will reveal that some, and maybe all, of the required infrastructure is already in place. Each situation will vary and dealers will have to take the responsibility of identifying their own requirements. For dealers that must add infrastructure, it can be done in phases as long as the individual phases are directed toward a complete solution. In the detail that follows, the outline for a basic dealership network is drawn. Using these guidelines, a dealership can determine if additions or changes will be needed.

Figure 2. OEM Vision



I.VII. BENEFITS TO DEALERS

There are many benefits for dealers from the migration to Internet-based applications and the use of common standards across OEMs. Many of them, however, are dependent on two factors:

- Business-class Internet connection.
- Good standards-based network design.

Dealers are encouraged to review their Internet connection as well as the overall network design in order to maximize these benefits:

Benefits of Internet Migration.

- Better understanding and more control over network design.
- Ability to select from a larger pool of technology vendors.
- Long-term reduction in network complexity.
- Use of open standards - not dedicated-OEM infrastructure, but flexible Internet infrastructure that is open to other OEMs and consistent with the National Automobile Dealers Association (NADA).
- Potential lower cost through reduced complexity and redundancy.
- Allows access to web-based applications.
- Increased speed of new application upgrade and deployment.
- Enables dealership personnel to access any application from any PC in the dealership.
- Enables public Internet access from all points of the dealership.
- Facilitates data sharing within the dealership.
- Increased potential for interaction with partners and customers.
- To provide continuity over time, OEMs will create a governance body to ensure that all additions are in accordance with these agreed-upon standards.

I.VII. DISCLAIMER

Any company name, application, website link, or technology reference mentioned in this document should not be considered an endorsement by the OEMs or by STAR unless that endorsement is expressly stated. This document provides a basic specification or guideline for dealers to establish Internet communication.

EXECUTIVE SUMMARIES

II.I. Overview

The executive summaries for the Dealership Infrastructure Guidelines (DIG) are designed to help dealers understand the purpose of each chapter as it relates to the dealership infrastructure. These summaries are a simplified clarification of each section including a high level overview. For further information, you will need to review each chapter in detail and visit the glossary for an explanation of terms.

Chapter 1, *SERVICE LEVEL AGREEMENTS*

Service Level Agreements (SLAs) are an important part of dealer/vendor relationships. SLA documents are used to assist both parties in understanding the guidelines and requirements relating to the service the vendor is supplying. An SLA can be used for both internal and external services. For this document we will focus only on the external aspects.

Chapter 2, *TRADITIONAL NETWORK INFRASTRUCTURE*

Consolidating a dealership network infrastructure across franchises reduces the complexity and cost of supporting proprietary solutions by decreasing equipment requirements, maintenance responsibilities, and other related expenses. The configuration of the network will vary depending on desired functionality and the number of clients. Several types of network configurations are discussed in the chapter.

The dealership is expected to maintain an Ethernet LAN according to computer industry standards. The network must be Ethernet based on the standard speeds allowed. On any given segment of the LAN, the speed is limited by the slowest component. Equipment should be securely mounted on racks or shelves with precautions taken to avoid damage due to poor power conditions and changes in temperature and humidity.

Chapter 3, *NETWORK DESIGN FRAMEWORK*

Routers, switches, hubs, web caches, and network interface cards all combine with building wiring to connect computers. They work together providing a solid backbone for the LAN and the connection to the Internet.

Web caching is the temporary local storage of web objects such as Hypertext Markup Language (HTML) documents, images, audio files and video files for later and faster retrieval. A local cache solution delivers frequently requested content faster. Caching may eliminate the need for additional bandwidth.

The core elements of all dealership networks are the same. The specifics of each individual design is dictated by the complexity of the dealership. If computer equipment requires segregation from the rest of the network, accommodations must be made in the plan. Equipment may vary by quantity, capacity, and capability but the role and function of the network remains the same. This chapter provides details on the individual core pieces used in the design framework of dealership networks.

Chapter 4, *NETWORK SERVICES*

This chapter is about maintaining the dealership's network and ensuring that the network infrastructure supports the dealership's business needs. Network Services goes beyond the designing and building of a

LAN, as this is only a small portion of systems integration. It is important to select a competent maintainer. If an Internet Service Provider (ISP) cannot or will not support the equipment, it is recommended that an outside resource be contracted. The dealership places a great deal of trust in this resource and people with the necessary skills are not found in many dealerships.

The dealership needs visibility and control of the network infrastructure. Use components that not only meet price points but can also be quickly serviced and managed. Beware of services that are bundled into an appliance. While deployment is easy, the dealership LAN may be vulnerable to loss of service.

Network services can be viewed as a stack of protocols and software that must be managed collectively after the network is initially installed. Managing the exchange of data between necessary parties on an ongoing basis requires considerable effort.

Chapter 5, *PRIVATE AND VIRTUAL PRIVATE NETWORKS*

Private networks are point-to-point circuits that connect two locations. Traffic is safe and reliable because there is no possibility of interference from outside sources except physical wire taps. Because private networks are closed they limit contact with other networks. Private networks tend to be more expensive because the communication medium is dedicated.

A Virtual Private Network (VPN) is a private data network that makes use of public telecommunication infrastructure. A VPN can use public switched networks or, in some cases, the Internet. Privacy is maintained by using software-based tunneling protocols or hardware-based gateways. Because a VPN has inherent risks that do not exist with a private network, VPNs add a supplemental level of security by encrypting data before sending it through the public network and decrypting it at the receiving end.

Chapter 6, *WIRELESS NETWORKS*

Use of wireless networks has become more popular with the advances in wireless technology. Wireless LANs enable network communication and connectivity without the physical restraints of hard wired cabling. Wireless technology can be especially useful in building-to-building communication or connecting a computer to a network where wired cabling is difficult or expensive. Wireless networks enable users to move freely from office-to-office, building-to-building and location-to-location while still accessing network resources and the Internet.

There are currently two primary standards used in the deployment of wireless communications, 802.11g and 802.11b. (Watch out for 802.11n) Most laptops and PCs are preconfigured for wireless compatibility. Users without this feature are required to install a wireless network interface to enable access to a wireless network. Wireless solutions are inherently less secure than wired connections; therefore, it is imperative that heightened security measures are provided. Wireless encryption, firewall configurations, and password authentication are strongly recommended when using Wireless Networks. Watch out for WEP (wireless encryption protocol); there is easy availability of tools to get around the keys.

Chapter 7, *DEALERSHIP SECURITY*

The most important element of a good network design is also the most often overlooked – security. Too often security outlays are considered expensive, never ending line items that can be trimmed or eliminated when looking for budget reductions. Quite the contrary, security spending is a strategic investment that protects the business.

There is no single fix all ingredient to the formula for complete network security. Some networks simply place a firewall device between themselves and the Internet and assume that all is safe. In reality, even

the best firewall provides minimal help if its configuration is weak or out of date. A proactive security approach helps avoid problems by layering people, hardware, and software to create reasonable and safe protections around the network.

Chapter 8, *DEALER MANAGEMENT SYSTEMS*

This chapter covers the OEMs' vision of a single LAN in the dealership controlled by the dealer and enabled for Internet access. Today's dealership environment may contain multiple LANs. The goal in developing the DIG was to help dealerships transform their network LANs into a single, Internet-enabled LAN.

A checklist to help dealerships evaluate their current infrastructure and future needs is located in the Appendix. One of the main premises of the DIG is that the dealership maintains control and ownership of its LAN. Plans are being developed to enable all applications to be accessed from the single dealership LAN, whether the application is from an OEM, DMS Provider, or provided by a third party supplier. A dealership that establishes control over its LAN gains greater flexibility and freedom to enhance the LAN with applications from a variety of sources.

Chapter 9, *CLIENT HARDWARE REQUIREMENTS*

Choosing the right hardware is the first building block of a dealership network. Understanding OEM requirements for computer hardware and going just a few steps above and beyond those requirements could significantly improve the dealerships bottom line.

Take action to implement these four simple, yet effective methods:

- **Surge Protection-** Providing surge protection for PCs and network devices is the easiest and most effective way to extend the life of the equipment and avoid expensive downtime.
- **Network workstations using common, modern methods -** Use the STAR DIG to implement a computer network with common and standard devices and protocols. Sharing internet connections and printers can directly improve the dealerships bottom line.
- **Provide virus protection -** Virus protection software helps prevent expensive downtime of systems.
- **Maintain reasonable and useful equipment warranty services -** When negotiating for warranty services, keep in mind that the average PC life is three years and onsite repair services are less disruptive and can be less expensive.

Chapter 10, *HARDWARE PERIPHERALS*

There are many factors to consider when choosing items such as printers, faxes, uninterruptible power supplies, and back-up and recovery systems.

This chapter is a compilation of checklist, considerations, and best practices regarding the implementation of network devices and computer peripherals in the office environment.

There are six basic considerations for selecting any add-on to a computer network. They are:

1. Ease of Use
2. Reliability

3. Performance and Speed

4. Cost of Ownership

5. Depth of Feature Set

6. Implementation Issues

Chapter 11, *DEALER DESKTOP MANAGEMENT*

Because computer technology has advanced, it is less likely that problems with a system originate with the flaws in the computer's hardware. The introduction of malicious software to systems from the Internet and internal sources is one of the biggest threats to information security and computer productivity. Malicious software is defined as any software that attempts to subvert the confidentiality, integrity or availability of a system. Spyware, viruses, worms, logic bombs, trapdoors, and Trojans are all considered malicious software. These unwanted intruders cause a variety of problems from slowing computer-processing speeds to outright stealing of privileged information, which could lead to liability.

The industry is dependent on computer technology to conduct business; protection MUST be a priority. Desktop Management is a combination of products and solutions (i.e. Virus software, Anti-Spyware, Patch Management) that helps keep the desktops running at peak efficiency. These products do many things including protecting your PC from viruses and other malicious software in addition to detecting patch application and operating system vulnerabilities.

Chapter 12, *MULTIMEDIA DELIVERY*

This chapter covers the topic of available methods of information distribution to dealership employees. With today's ultra-competitive and rapidly evolving business climate, it is essential for dealerships to train and support staff with the latest and most advanced information available. Multimedia Delivery is the distribution of multimedia content (training material, marketing programs and competitive analysis) to users. Multimedia is available from numerous sources with technological advances making access to this content continually easier and more convenient. Whether the content is locally created, comes from OEMs or third party developers, today's dealership has access to a wide array of competitive information for its employees.

Each dealership must devise a strategy to deliver the information contained in the ever growing number of content delivery options. The strategy prepares dealer management for associated costs and logistics when implementing successful content delivery systems. The strategy addresses items such as what content the dealership intends to provide, where employees are able to receive that information (at the office, at home, in an offsite classroom, etc.), which delivery methods the dealership's OEM's support (broadcast video, Internet, DVD, etc.), content reusability and the deployment of infrastructure needed to deliver content.

Understanding the benefits and limitations of these options further enhances the learning experience and training goals for the dealership. A Multimedia Delivery strategy guides the dealership in achieving its goals and avoiding unexpected costs.

Chapter 13, *INTERNET ACCESS METHODS*

With the growth of the Internet, dealerships as well as OEMs are migrating many applications and communications to the Internet. Before purchasing any internet connections, it is important to understand the

present and future needs of the dealership. Ask important questions such as: Do I want to host my own email? Do I want personnel to remotely connect from home? What kind of uptime am I willing to pay for in an SLA?

There are a wide variety of ways to access the Internet ranging from dial-up, and cable connections to leased lines (T1, frame relay), satellite, or Integrated Services Digital Network (ISDN) products. There is widespread availability of these methods. Their capacities have range from low-speed 28.8Kbps dial-up to moderate speeds of 1.5Mbps leased lines. Cost will vary depending on the type and speed of access.

An Internet solution is based on the overall strengths and weaknesses of each access method. It helps to decide which Internet connection method is right for the dealership. Individual decisions are guided by availability of service, capacity requirements, SLAs, and cost for the dealership. Products with high ratios of bandwidth to costs, such as DSL, are usually the most attractive but may not be available in some areas requiring the use of a more traditional service. Because the market constantly offers new products, avoiding long-term contracts allows dealerships to take advantage of new products or downward shifts in current product pricing.

Chapter 14, *INTERNET CONTENT FILTERING*

Many companies take steps to monitor and limit network usage by implementing Internet content filtering products. These products can be strictly software or a combination of hardware and software. Typical sites that may be considered for filtering include those that carry illegal copyrighted material, adult content, games and high bandwidth audio and video streams. Restricting access from certain Internet sites poses a challenge due to the sheer number of new sites that appear daily. For that reason, many content filtering vendors constantly update lists that categorize the types of Internet sites. These updates are usually offered as a subscription download service. Filtering products provide reports about the usage patterns that exist in a dealership. Usage pattern monitoring is a proactive tool to mitigate the risks and cost of sensitive information losses, bandwidth overload and employee issues.

Chapter 15, *SAFEGUARDING CUSTOMER INFORMATION*

Safeguarding Customer Information is not just good business practice; it is the law. Violations can result in stiff penalties. The Gramm-Leach-Bliley Act (GLB) and the Federal Trade Commission’s (FTC) privacy rule (Privacy Rule), obligate dealers to disclose to their finance, lease and insurance customers how their information is used and shared. The new safeguard rules have three primary objectives:

- First, insure the security and confidentiality of the dealership's customer information.
- Second, protect against any anticipated threats or hazards to the security and/or integrity of the dealership's customer information.
- Third, protect unauthorized access to or use of the dealership's customer information that could result in substantial harm or inconvenience to any customer.

A link to a web site containing an NADA guide to implement the safeguard program is provided in the recommendation section. []

Chapter 16, *DISASTER RECOVERY AND BUSINESS CONTINUATION*

As business relies more on technology to gather data and perform daily functions the importance of protecting that process becomes critical. It is not enough to have just a backup of necessary information. A

dealership must have a plan in place to ensure that information can be restored. Without the proper plans and people in place to perform these tasks, a dealership could suffer critical loss in the event of a disaster whether it be technical or natural.

???

The DIG recognizes that technology is constantly changing and expanding. The technology watch chapter highlights new devices, systems and concepts that are beginning to impact or will have an impact on dealerships in the future.

ROLES AND RESPONSIBILITIES

III.I. Overview

This chapter explains the responsibilities that exist when beginning to implement a new dealership infrastructure. If each party delivers on its area of responsibility in a timely manner, the installation and ongoing support process should be successful.

OEMs will:

- Provide support through each OEM's help desk for OEM-specific applications and infrastructure.
- Provide limited assistance and direction on Local Area Network (LAN) integration.
- Provide limited assistance and direction on Internet connection.

The dealer will:

- Provide a single point of contact (Project Leader) and an alternate for the OEMs and suppliers.
- Sign an Acceptable Use policy if required by OEM.
- Provide a secure network environment (see Chapter 2, *TRADITIONAL NETWORK INFRASTRUCTURE*).
- Agree that there will be only one public Internet connection per LAN (due to security issues, routing complexity, troubleshooting, support issues, etc.) – this does not include backup connections to the Internet.

The dealer will be responsible for providing or procuring services to:

- Design, build, and maintain an Ethernet network infrastructure (Category 5 or 5E cabling standards, connectors, hubs, switches, network cards, etc.).
- Support the internal dealership LAN and the Internet browser and non-OEM applications.
- Integrate existing dealership LANs, additional PCs and LAN drops – according to individual OEM migration plans.
- Manage and support a router and firewall.

The project leader will:

- Review dealership needs and OEM specifications.
- Develop timelines for implementing changes.
- Assist dealer in selecting appropriate personnel to design and implement network.
- Perform quality audits and performance reporting.

Chapter 1. SERVICE LEVEL AGREEMENTS

Table of Contents

1.1. OVERVIEW

Service level Agreements (SLAs) are an important part of dealer/vendor relationships. These documents are used to assist both parties in understanding the guidelines and requirements relating to the service the vendor is supplying. An SLA can be used for both internal and external services. For this document we will focus only on the external aspects.

1.2. WHAT IS AN SLA?

An SLA is a legally binding contract that outlines, in detail, the product or services being provided to the dealership. It covers areas of services, support, availability, upgrades and legal.

1.3. WHEN SHOULD AN SLA BE USED?

Every service being provided to a dealer should be accompanied by an SLA. This allows the dealer to fully understand what will be provided setting expectations. The dealer is protected in the event that a service is not provided as outlined by the SLA; the service provider is protected against a dealer escalating expectations.

1.4. WHAT SHOULD AN SLA INCLUDE?

The SLA includes all the areas that are affected by outside support. These areas include detailed information about the service expectations.

Service

This is a description of what is being provided. For example, a Data Storage SLA states what data is being stored, what mechanism is being used to store the data, duration of storage , how to retrieve the data, who may retrieve the data, etc.

Hours of Export

Specifies the specific days and hours that data extraction will occur.. This is vital since extracting data during operating hours could negatively impact the dealer's system performance. These details should be specified and agreed upon between the two parties.

Location of storage

This is a detailed outline of the location of the data. It includes location of building, location within the building, hardware used, etc.

Support

The SLA details timeframes for support. Included are: response times for classes of issues; the normal hours of support; arranging off-hours (after hours and weekend) support; and any costs for support not included in the basic contract document.

Information Access

The SLA details the dealer's right to access the information including time restrictions. It details any outlined costs for access and should outline the process for getting that information. Any administrative burden associated with information storage or access, expected to be borne by the dealer, should be explicitly stated.

Downtime and Penalties

If the service is entitled to some downtime, the amount, for instance 2%, is specified here. When the service exceeds the specified downtime limit, the vendor is required to pay some penalty, such as discounting the monthly/yearly fees. The SLA should include information about what the service will do if downtime materially affects the service, i.e., the necessary information was not stored during the outage and a mechanism to address these issues.

Legal

This will cover any intellectual property, Legal Compliances, etc. It would be in the best interest of the dealership to have a legal representative review these areas.

Most vendors should have an SLA in place. There may be areas missing so make sure to review it and ask them to add any information that is not addressed.

In the event that a vendor does not have an SLA the dealer should request one be created. The dealer should feel free to create a SLA to be presented to the vendor. There are various websites and documents that can be utilized to help a dealer create the necessary details to be included in an SLA. Below is a list of a few websites that will assist in the creation of an SLA:

http://www.itil-itsm-world.com/

http://www.service-level-agreement.net/

http://en.wikipedia.org/wiki/Service_level_agreement

http://www.businesscontingency.com/checklist-sla.php

http://www.nkarten.com/handbook.pdf

Chapter 2. TRADITIONAL NETWORK INFRASTRUCTURE

Table of Contents

2.1. OVERVIEW

The primary advantage of upgrading the dealership's network infrastructure is to reduce the complexity and cost of supporting proprietary solutions previously required for each of the dealer's franchises. Consolidating the network infrastructure can contribute to the reduction of equipment requirements, maintenance responsibilities, and related expenses.

Every effort has been made to provide quality solutions within the economic scope of dealerships of all sizes. The following section contains information about the physical elements within the dealership network. These include wiring, hubs, routers, switches, and other network components.

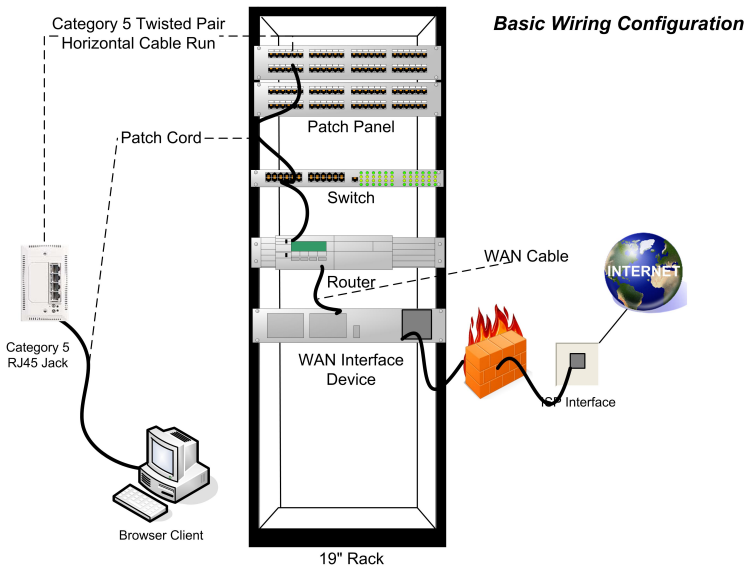
Defined within this section are installation guidelines for a dealership Local Area Network (LAN)and some minimum specifications and requirements for network hardware. Both dealership personnel and potential network suppliers must be familiar with network environments and with the information necessary to build a suitable network infrastructure. The network and its components must comply with industry standards.

Recommendations are given to ensure all equipment is reliable, upgradeable, and scalable. Overall, flexibility of the network is necessary to accommodate changing and emerging technologies, as well as to allow open integration with other OEMs.

The network must be Ethernet based with the standard speeds (100BaseT or 1000BaseT) allowed. However, on any given segment of the LAN, the speed is limited by the slowest component; e.g., using 100Mbps LAN cards with a 10Mbps hub will result in an overall network speed of 10Mbps.

The dealer is expected to build an Ethernet LAN according to computer industry standards (referred to as Category 5 standard). OEMs strongly recommend that this LAN have a central wiring repository where all cables runs are terminated on patch panels. It is strongly recommended that wiring hubs, switches, routers, and communications equipment are located nearby and that all equipment is securely mounted on racks or shelves. Precautions are required to protect this equipment from damage due to poor power conditions and changes in temperature and humidity.

Figure 2.1. Simplified Dealership Wiring



A sample wiring configuration is demonstrated above (see Figure 2.1, “Simplified Dealership Wiring”). This diagram represents the base configuration that allows a Personal Computer (PC) in the dealership to access the Internet. Dealer Management System (DMS) equipment, any satellite or OEM-specified equipment, and other dealership installed equipment comprising the remainder of the entire dealership network are not shown on this diagram.

2.2. WHAT IS NETWORK UTILIZATION?

Network utilization is the amount of traffic on the network compared to the peak amount that the network can support. This is generally specified as a percentage.

There are various times throughout the normal course of business when a network is busier, i.e., the network utilization is high. As a result, users experience a slow down when the network utilization is high enough. Response times grow greater than expectations preventing normal business processes from operating efficiently. Performance degradations are generally a nuisance but can become significant enough to result in lost revenues. It is important to understand the factors that can cause high network utilization and how to manage the network preventing it from negatively impacting the business.

Factors that can affect performance

- Infrastructure - The layout of the internal network and the devices attached to it impact network performance. A network is made up of interconnected components some or all of which are required for any given operation. A particular response depends on the response times of all of the components in-

volved. As a rule of thumb whenever a component of the network is more than 70% utilized, slowdowns will occur. If the component is highly utilized for long periods of time, the slowdowns turn into serious delays. The connection to the outside Internet can become a bottleneck when more interactions with the Internet occur than the service provides.

- Internal Usage - Some business-related processes require a significant amount of bandwidth under normal conditions. Data backups, teleconferences, VOIP phones, and even virus scanners can cause network utilization to become high, as a result, slowing other processes that require network resources to function.

- Non-business Related Activity - In many cases, non-core activities occurring within the business are found to be the culprit of high network utilization. Casual web surfing, Internet radio streaming, and viruses that have infected machines on the network can steal precious network resources and cause problems with critical business functions.

- Factors that affect network utilization and the performance of the network fall into a few major categories.

Table 2.1. Tools to Monitor Network Utilization

Service	Dealer w/o IT Department	Dealer w/ IT Department
Off the shelf single PC usage	X	
Off the shelf multiple PC usage	X	X
Server side	X	X

The type of software that you purchase will depend greatly on what the needs of the dealership are. Some of the keys items to consider when purchasing or outsourcing network utilization tools are:

- Current Problems - This could include lag on the network, network crashing or inconsistent network availability, or a possible virus.

- Future Problems - Make sure the product will support future plans, such as additional users, network changes, etc.

- Bandwidth monitoring - Can the tool monitor the bandwidth that is available (keep in mind this may not equal exactly what you signed up for. Many factors effect this number)

- Available features:

  - Collect top sites that users visit.

  - Collect information on the top users.

  - Optionally block certain sites or specific terminology.

  - Filters.

  - Alerts.

  - Provide enough detail to list ip addresses, etc. (this may be IT dept).

- Provide pinging (details).
- Catch and inspect packets off the line (wireshark).
- Network sniffing (who is using what).

In a situation where the network monitoring is outsourced, the dealership needs the option to monitor the reporting, change any network settings, etc. If these features are not available, the dealership should construct and SLA specifying a pre-defined list of report dates, etc.

Management

In an effort to reduce latency due to excessive traffic or other contributing factors it is important that certain steps be taken. For example, ensure a proper network infrastructure layout has been established. If that is not possible, review the current infrastructure and determine which areas can be enhanced or re-engineered to improve performance. Often, a single infrastructure bottleneck is found to be a significant source of performance issues.

In addition to setting up the infrastructure correctly the network will need ongoing maintenance and monitoring to ensure that other factors such as hardware/software failures, bugs, viruses or misuse of resources are not occurring. Many organizations have begun implementing policies restricting usage of Internet resources to minimize the impact of non-business related activity on the network.

2.3. VIRTUAL LOCAL AREA NETWORK

2.3.1. Overview

A Virtual Local Area Network (VLAN) (IEEE 802.1Q Virtual LANs) should be considered in environments where users are required to access applications and data from dissimilar networks, such as a dealership LAN, DMS LAN, OEM 1 LAN, OEM 2 LAN, etc. Deploying a VLAN often requires additional costs up front. However, long term costs may be reduced because of the flexibility and ease of management. A VLAN combines switches and routers to logically connect or isolate network segments according to some predefined criteria, such as job function. Some of the tasks of a VLAN are accomplished using switches alone (one big LAN). Without routers, containing broadcasts and adding security becomes difficult, if not impossible. A VLAN also overcomes the difficulty and inflexibility of managing hard-wired connections. When moving a device on the network, such as a PC or printer, no rewiring is required in most cases.

2.3.2. Planning for VLANs

OEMs recommend integrating multiple LANs that require different IP addressing using a router and an Ethernet switch that fully supports IEEE 802.1Q VLANs. This provides the flexibility to integrate additional LANs later without purchasing extra Ethernet interfaces for the router. The equipment has the ability to support multiple VLANs on a single router interface from a single switch port and maintain separation of Ethernet collision domains while routing the IP packets among VLANs. These capabilities may be combined into one device called a layer 3 switch. A layer 3 switch can replace both a router and a layer 2 switch, but is usually more expensive.

VLAN capabilities can be incorporated in the Internet (main dealership) router. Adding isolation routers between LANs and the dealership's network switch are unnecessary for security when the proper Internet firewall guidelines are followed. Additional hardware adds complexity, cost and may reduce performance.

It is extremely important to document both the physical and logical layouts of the dealership's network environment. This greatly reduces the time needed to troubleshoot problems and make changes or additions to the network. Clear, concise documentation is best kept in a centralized location. The documentation includes:

- Support contact information for each LAN.
- Support contact information for the Internet Service Provider (ISP).
- Copies of all support contracts.
- All IP address information (Address pools, Domain Name Server (DNS) addresses, and default gateways for each LAN and the ISP).
- Demarcation points for each support organization.

Keeping the documentation up to date is important.

In addition to the layouts and support information, the Ethernet switch ports should be clearly labeled with IP address information as well as VLAN membership information. Verify that the LAN provider provides and maintains a copy of this documentation.

The following sections include a description of the information needed to implement the multiple LAN environments. Gathering the items in the section on Network Design Framerwork routers and Required ISP Information is required regardless of whether the network design is done in-house or by an outside provider.

2.3.3. Required LAN Information

For each LAN in the dealership, use the site survey forms in the Appendix A, *Dealership Needs Assessment* to collect and document the following information:

- Support contact information.
- IP subnet address and subnet mask.
- Existing default gateway IP address for client PC's.
- Existing Client DNS requirements.
- Identify the connection point on the LAN (router interface or switch/hub port).
- IP address on the LAN for the dealership's network router interface. (Obtain from ISP)
- Dynamic Host Configuration Protocol (DHCP) information.

  Reserve IP address for DHCP server on the LAN (could be the router)

Reserve IP addresses for File Servers
Reserve IP addresses for Printers
Reserve IP addresses for other servers or devices

2.3.4. Required ISP Information

The Internet Service Provider must supply the following information:

- Support contact information.
- IP subnet address and subnet mask.
- IP addresses for Demilitarized Zone (DMZ) if needed. (Public Internet IP addresses space).
- Public DNS server addresses (two minimal).
- Login information if needed for the router/firewall to establish connectivity.
- Identify the demarcation point and the connection type (modem, router, bridge, etc.) With DSL, Satellite, Wireless, and Cable Modem, it may be an Ethernet port. With T1 or Frame Relay, it may be a V.35 interface on a Channel Service Unit /Data Service Unit (CSU/DSU) or it could be an Ethernet port on an ISP supplied router.

2.3.5. Design and Implementation Considerations

When designing and installing VLAN environments, the following items deserve special consideration:

- Review the design information gathered earlier. Review for possible IP address conflicts.
- Again AD will have issues with not being your networks DNS. This setting will be in the DHCP server.
- Document and label Ethernet switch ports as to which VLAN they are a member of and include IP address information as well.
- Identify and order Cat5E cable drops needed to connect each LAN with the Ethernet switch. Be aware that crossover Cat5E patch cables may be needed when connecting from switch to switch or hub to switch.
- Configure the router interface for the Internet transport.
- IP information.
- NAT (Network Address Translation) or PAT (Port address Translation. Wikipedia provides a good introduction to NAT, PAT and allied concepts. See also: http://computer.hhowstuffworks.com/nat3.htm
- Security (recommend firewall on this interface).
- Configure the router interface for the dealership DMZ if needed.
- Public Internet IP address space will be needed.

- Security (Firewall rules for the DMZ will need to be implemented).
- Configure the interface for the Ethernet switch.
- Primary IP address and subnet mask.
- Secondary IP address and subnet mask for each VLAN.
- VLAN configuration and naming for each VLAN.
- NAT for each LAN going to the Internet.
- DHCP network and DHCP helpers for each VLAN.
- Configure VLANs on the Ethernet Switch.
- Define VLANs by IP address.
- Assign ports to VLANs.
- Ensure that the port connecting to the router is a member of all the VLANs.
- Label and document everything.
- Configure static IP routes.
- Default route to the Internet (transport/ISP interface).
- Other routes as needed.
- Test for proper, configuration and functionality.

2.4. MULTI-BUILDING/LOCATION NETWORKS

A business that has multiple locations can often benefit from leveraging resources such as computer data, business applications, servers, and other devices through a network connection between buildings. Additionally, services such as centralized voice, video, faxing, administration and broadband Internet may be utilized by an entire organization. The increased capabilities and benefits will often offset the expense of these connections. Campus Networks and Wide Area Networks (WAN) are two types of networks, which allow sharing of networked resources between buildings or remote locations.

If there is a desire to access these resources from another location, it must be determined whether the business need warrants the cost of the connections. There are elements to consider when establishing the value in connecting each location. Consider the following when deciding:

- Connection of business applications (OEM, DMS, Accounting, Parts, etc.).
- Central services: faxing, printing, IT administration.

- Sharing a broadband Internet connection.
- Sharing and transferring files.
- Inter-office email and Intranet.

Each location needs to be individually evaluated for connectivity and bandwidth requirements. Factors such as the number of users running remote applications or the amount of data transferred can help determine bandwidth requirements. If connection reliability is critical, then Service Level Agreements (SLAs) will be of great importance.

A qualified supplier should be able to provide assistance in making an accurate estimate of business needs. An approach to finding suppliers might include contacting local suppliers of phone services, long distance service, network services, telecommunications equipment, and web related services. It is recommended that credentials, certifications and references be obtained.

Many factors should be taken into account when determining connection requirements:

- Bandwidth
- Latency
- Scalability (Ability to easily increase bandwidth)
- Cost vs. Performance
- Service Level Agreements see Chapter 1, *SERVICE LEVEL AGREEMENTS*.

2.4.1. Campus Network

A Campus Network exists when the grounds on which the buildings reside are contiguous. This includes right of way permission to use the span between locations to install buried or aerial cabling. See the Section 6.4, “WIRELESS LAN SECURITY” for more information. Point-to-Point wireless connections offer another alternative when buildings are within range. All of these connections are private and typically created using fiber-optic, copper, or wireless mediums. Usually campus network configurations occur in smaller geographical areas. Common examples of campus network implementations are hospitals, universities and dealerships.

2.4.2. Wide Area Network (WAN)

A WAN is the extension of a network spanning across a geographical area in which right of way privileges do not exist or wireless is not an option. A WAN environment can also accommodate users that are mobile or spread out over a broad region. WAN connection technologies include T-1, OC3, DSL, cable, or fiber modems and finally satellite.

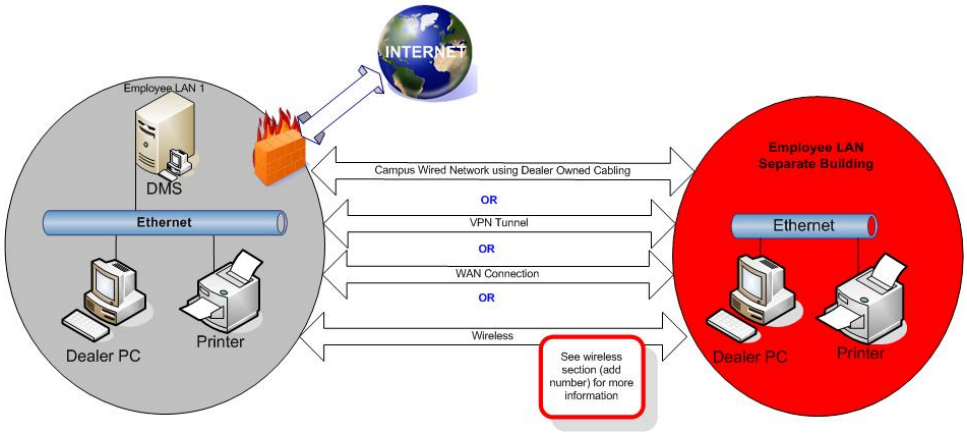
2.4.3. Virtual Private Network (VPN)

A VPN is a method of providing secure communication over the Internet or other IP networks. A VPN can provide significant cost savings when applicable. See the Chapter 5, *PRIVATE AND VIRTUAL PRIVATE NETWORKS* for more information.

2.4.4. Multi-Location Recommendations

If a business has "right of way" and/or wireless is a viable option, then a Campus Network should be considered due to lower recurring costs and generally better performance than a WAN. In some instances the local telephone company will grant the right of way and install or lease the necessary cabling in order to establish a campus connection. If there is no right of way, or wireless is not an option, a WAN or VPN should be considered. The choice of connection method is based on business requirements, available technologies, performance and associated costs. If cost effective broadband Internet access is available from multiple locations, an Internet VPN may be preferable. In some scenarios, a hybrid design combining campus, WAN and VPN technologies may be the best solution.

Figure 2.2. Campus Network Options



As with all technologies, multiple proposals are recommended for network solutions. While evaluating solutions from vendors, it is advisable to get network diagrams that indicate both logical and physical layouts. The solutions should be detailed in order to properly compare cost, technologies, bandwidth, and performance variables. A bill of materials, statement of work and maintenance contracts should be included with each proposal. Because technology is changing so rapidly it is strongly recommended that data communications contracts be limited to one year if possible.

2.5. Multi-OEM Locations

OEMs are standardizing their applications to run over the Internet diminishing the need for custom OEM hardware, software and network requirements inside the dealership. During the transition period, while OEM applications migrate to the Internet, provisions MUST allow for legacy network paths. Additional OEMs and dealership system providers may have their own requirements inside the dealerships. To avoid potential network communication problems, a single point of exchange is employed to manage traffic. The OEMs see that exchange point as the network switch. The dealership must understand that the multiple-OEM dealership integration will become complex in the short term until all applications are migrated to the Internet. A competent individual or third party is required to manage IP addressing and some of the more intricate aspects of networking (e.g., VLANs)

Each dealership needs a path to the Internet that goes through the Internet router and firewall controlled by the dealership. Other paths to the Internet must be similarly controlled or isolated from the dealership's

private network. Any system providers that accept this view can join the standard by attaching equipment to the delearship's switch, thereby accepting dealership control.

2.6. Network Infrastructure Recommendations

Table 2.2. Infrastructure Cost Estimates

Item	Description
Local Area Network	Ethernet Based.
Speed	100Mps (100BaseT) or 1000Mps (GigB) for new installations or 1000Mps (GigB).
Wiring	Minimum Category 5 standards Category 5e for new installations.
	Fiber optics cable used inside on long runs (over 295 feet) and between buildings where possible.
	Wireless methods can be used (with caution) where wired options are not possible or too expensive. New wireless equipment should meet 802.11b standards.
Equipment	All dealerships will need a router and a network switch.
	All equipment should be certified to meet current industry standards.
Traffic	All Internet traffic should be routed through a single point (router).
	The segmentation of dealership or OEM LAN's should be controlled at the network switch.

2.7. USEFUL WEBSITES

Implementation Information

- www.cisco.com
- www.csrstds.com
- www.ietf.org
- www.ieee802.org

Chapter 3. NETWORK DESIGN FRAMEWORK

Table of Contents

3.1. OVERVIEW

The configuration of the network comes from a detailed network design plan. This plan should take into account any router, switches, hubs, cabling and other network interface-related items. The complexity of the design will depend on the needs of each dealership. If there is a need for network segregation to accommodate different vendor equipment or additional user needs this must be documented in the plan from the beginning. While equipment quantity and capability may vary, the role and function of the network will essentially be the same for most dealerships.

In addition to the general network design that is needed, the dealership may want to give access to guests. It is important that this access be segmented from the rest of the dealership LAN.

3.2. WIRING STANDARDS

3.2.1. Data Cabling

For existing installations, all connectivity products (this includes: copper cable, jacks, inserts, modular plugs, patch panels, patch cords, etc.) must meet or exceed TIA-568-A Category 5 standards. All Category 5 cabling is certified to support speeds up to 100Mbps. Many companies routinely use it for faster transports. New wiring installation should meet Category 5e standards. This newer, enhanced standard is certified to support speeds up to 1000 Mbps. The use of Category 3 UTP cable for data purposes is not advised, as it does not support newer technologies like 100BaseT. Though this section references TIA-568-A category 5 and 5e standards, when the majority of the dealership's cabling is scheduled for replacement include Category 6 cabling in the evaluation. Category 6 cabling is suitable for use with 1000BaseT (gigabit) Ethernet and is backward compatible with 10BaseT and 100BaseT, providing room for later improvements. See the http://www.levitonvoicedata.com link for additional information on Category 6 cabling.

Installation must be performed by certified installers and done so in accordance with TIA-568-A Category 5 standards. No horizontal cable runs should exceed 90 meters (295 feet). Cable runs must not be installed near or parallel to anything that may produce electromagnetic interference (EMI), such as fluores-

cent lights, electric motors, etc. It is also suggested that a few feet of "service loop" is left for future serviceability, moves, additions, and changes. All cables and jacks (wall and punch panel) must be labeled clearly. Identification numbers should match a wiring plan that is kept near the central wiring location. It is a good idea to keep a copy of the plan in a file as well. Both copies should be updated whenever any wiring is added or changed.

The main distribution frame/intermediate distribution frame (MDF/IDF) end of each cable run should be terminated on a Category 5e patch panel or an organized jack/insert system. The workstation end of each cable run must terminate on a Category 5e 8-position jack. All terminations must be compliant with TIA-568-B wiring configurations. All inter-connections and cross-connections must be made using Category 5e patch cords. Lengths of said patch cords should comply with TIA-568-A Category 5e standards. Copper Category 5e cable should not be used outside of buildings or to connect multiple buildings. In this case, fiber optic cable or wireless connections are viable alternatives.

3.2.2. Fiber Optic Cabling

Fiber optic cable is highly recommended in place of data cable runs when the length exceeds 600 meters (approximately 1200 feet) in a campus environment or when connecting buildings together with right of way allowed. A minimum of four strands of multi-mode 62.5/125 microns is required. Extended distances or the implementation of gigabit Ethernet may require the use of single-mode fiber optic cabling. The environment in which the cable is installed will determine the type of jacket it requires. Plastic flexible tubing should be used when installing fiber optic cable if conduit is not available.

All cabling must be dressed into the MDF/IDF in a secure manner, in order to restrict movement. Terminations should be made with standard ST or SC-style connectors. Cables should terminate at a fiber patch panel. Fiber optic patch cords should be used to connect the patch panel to the Fiber Distributed Data Interface (FDDI) hub or other device. Fiber-to-copper transceivers may also be needed.

3.2.3. Building Codes

All local, state, and federal building, fire and safety codes, rules, regulations, statutes, and laws must be strictly adhered to. Plenum-rated cable must be used in all areas where required. These codes may also require that cable runs not touch or be fixed to anything that is not part of the permanent structure, such as drop-ceiling grids and electrical conduit.

3.2.4. Testing

All installed drops must be tested and certified. All cables tested must pass in accordance with TSB-67, TSB-95, and Category 5e guidelines. An electronic copy as well as a certified printout of the test results signed by the technician should be requested by the customer contact.

3.2.5. Hubs and Switches

A hub is one of the most basic elements of a LAN used to connect computers, printers, and other network components. Any device connected to a hub shares its bandwidth with all other connected devices. This is known as a shared segment or single collision domain. When there are multiple heavily used devices connected to a hub, many data collisions occur and users will notice degraded performance. This type of environment is not recommended for most applications. However, some computers that are infrequently

used, or that produce a minimal amount of traffic, such as an infrequently used printer, can be connected to a hub to keep hardware costs down.

Generally, switches are replacing hubs in LAN environments because they provide dedicated bandwidth to each device on a port, whereas hubs do not. Switches decrease network congestion, increase bandwidth, and isolate collision domains. They essentially prevent connected devices from "hearing" data traffic destined for other devices. Switches can be used to segment the network logically to provide maximum efficiency. Servers, routers, and high-volume users constitute much of the network traffic. Therefore, each device may warrant its own port on the switch. In a large environment, it is preferable to use a managed switch, as opposed to a non-managed switch, to aid in troubleshooting. Note that when replacing hubs with switches, you should upgrade the speed of 10Mb hubs to 100Mb switches.

Listed below are some general guidelines for selecting this equipment:

- Devices must match the IEEE 802.3 specification for 100baseT and should have RJ45 interfaces for twisted-pair connections.
- 100 or 1000 Mbps devices should be used in areas where a migration path is planned.
- Connection of multiple hubs and/or switches should be done in stacks without adding hops. This is achieved by connecting the back plane of the hubs via a proprietary cable instead of cascading them with patch cords using standard ports.
- If hubs are cascaded (daisy-chained) using crossover cables or ports, it should only be done with fewer than five on a particular LAN segment.
- It is suggested multiple hubs be connected to a switch in a star topology for LANs with moderate to heavy traffic volumes.
- Large LANs or campus environments may require FDDI, asynchronous transfer mode (ATM), and/or Gigabit Ethernet interfaces.
- Managed devices should support industry standards such as Simple Network Management Protocol (SNMP) and Remote Network Monitoring (RMON).
- Devices should be stackable or rack-mount style for neat, safe, and uniform installation
- Switches with VLAN technology should be used for internetworking environments.
- Devices with redundant power supplies are recommended to help minimize potential downtime.
- Wireless devices should be IEEE 802.11n compatible.

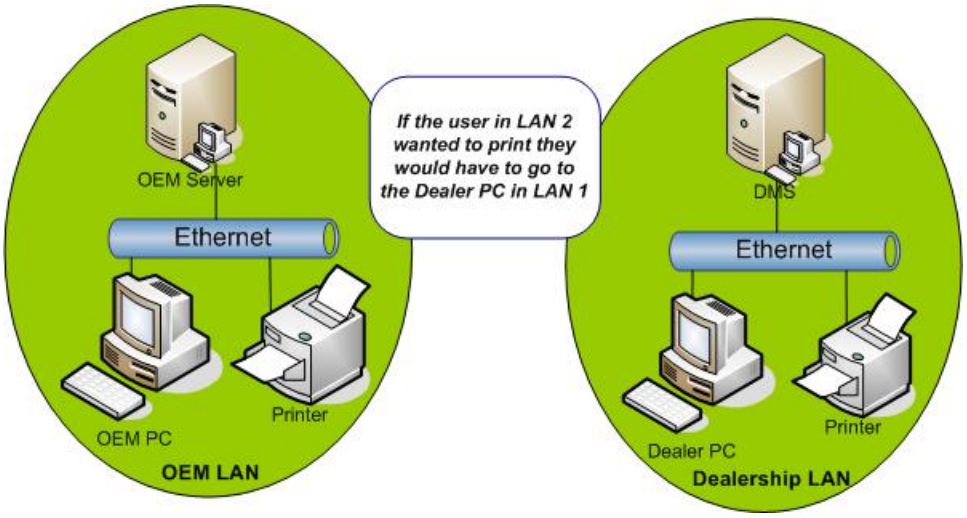
3.2.5.1. Layer 3 Routing Functionality

Layer 3 routing functionality allows computers from different networks and sub-networks to communicate. In dealerships, layer 3 routing may be used to connect an OEM LAN, dealership LAN, and DMS LAN to the Internet and helps enable the "only one computer per desk" goal.

While layer 3 routing functionality is actually available in different devices, including routers and switches, for the sake of simplicity this document will use the term “router” hereafter.

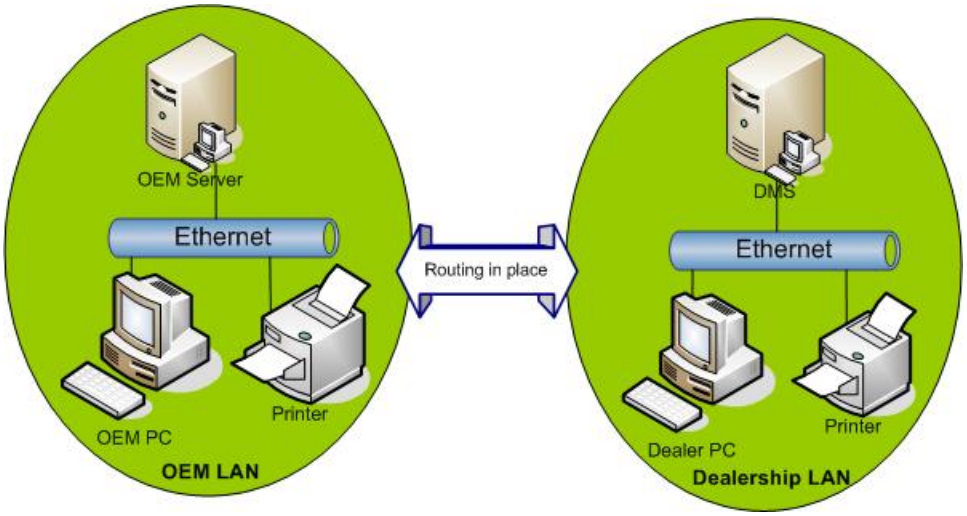
For example, if users on network 1 who perform accounting and printing functions need to access warranty information from a server on network 2, and no routing is available, they must use another computer that is on network - likely a second computer on their desk. (see Figure 3.1, “NONrouted LANS”)

Figure 3.1. NONrouted LANS



The above scenario is avoided if network 1 and network 2 are connected to a router to pass traffic between the networks. (see Figure 3.2, “Routed LANS”)

Figure 3.2. Routed LANS



Routers with logical sub-interfaces contained on a single physical Ethernet interface can route traffic between sub-networks that exist in a switched environment. This allows traffic to pass or be filtered depending on the situation. Routers with multiple physical Ethernet interfaces can be used for non-switched and switched environments. Use routers with these capabilities to communicate between different sub-networks in a local environment.

Listed below are some general guidelines for selecting this equipment:

- Routers must support Internet protocol (IP).
- Routers should support Network Address Translation/Process Analytical Technology (NAT/PAT)
- Routers should support Dynamic Host Configuration Protocol (DHCP) as a server and a client.

3.2.5.2. Ethernet Network Interface Cards (NIC)

Any device connected to Ethernet LAN must have an Ethernet card. Routers, switches, and servers always have an Ethernet card. When purchasing a new PC, ensure that Ethernet functionality is included, and if not one will need to be included. The guidelines that follow are valid for all Ethernet cards, regardless of whether they are integrated into the main system board or installed separately. General guidelines for purchasing a Ethernet card:

- Devices must match the IEEE 802.3 specification for 10baseT, 100baseT or 1000baseT (GIG Ethernet).
- Peripheral Component Interconnect (PCI) cards are preferable when compared to Industry Standard Architecture (ISA) because they offer greater throughput and are easier to install and configure.
- NICs must have a RJ45 interface for a twisted-pair connection.
- Onboard light-emitting diode (LED) status indicators to allow for easier troubleshooting of connection problems.
- Wireless NICs should be IEEE 802.11b/g/n compatible.
- Certification of interface cards by the operating system suppliers is highly recommended.

3.2.5.3. Equipment Certification

All equipment should be a brand produced by a reputable manufacturer with a history of quality merchandise. All equipment should be accredited or certified by one or more of the following organizations and agencies:

- UL Underwriters Laboratory.
- CSA Canadian Standards Association.
- ISO International Standards Organization.
- IEEE Institute of Electrical and Electronic Engineers.
- CCITT Committee to Consult on International Telegraph and Telephone.
- ITU International Telecommunications Union.

3.2.5.4. Controlled Environment/Equipment Care

A controlled environment is necessary for LAN equipment. Most service providers require a controlled environment as a condition for honoring warranty claims or service contracts. OEMs recommend the following guidelines to maintain the equipment and help prevent network outages:

- Do not stack equipment in a way that prevents heat dissipation or contrary to manufacturer recommendations.
- Do not block cooling fans.
- Do not place equipment in dusty environments.
- Do not place equipment or run wiring near anything that generates vibrations or strong electromagnetic fields (e.g., air-conditioners, welders, transformers, etc.).
- Do not switch devices off and then on rapidly. Wait 10 seconds before turning something back on.
- LAN equipment should be installed in a secure area that provides controlled temperature and humidity.
- Routers, switches, and other LAN devices should be installed on a Category 5-compliant rack or cabinet within close proximity to the horizontal cabling system.
- Racks should be anchored to the floor or mounted to a wall in a secure fashion per manufacturer's specifications.
- A wire management system should be used to keep the cross-connections of all devices neat and serviceable.
- All equipment, ports, jacks, and wiring should be properly labeled.
- All AC electrical outlets should be connected to dedicated circuits. Qualified licensed electricians must perform electrical work.

Chapter 4. NETWORK SERVICES

Table of Contents

4.1. OVERVIEW

The designing and building of a local area network is only a small part of the work that is involved in actually using the network. Managing the flow of traffic and the usability of the network will take more effort over time. Address schemes will need to be designed and routing tables set up accordingly. Some of this work is completed when the network is first set up. Barring any equipment failures, it may not need to be done again. However, even small networks need oversight on a regular basis. This is minimized if dynamic tools are used to assign network addressing and to resolve those addresses. The Internet Service Provider (ISP) may insist that these tools be used for the Internet connection. Even more benefits are seen if they are used inside the dealership as well.

The kinds of skills needed to perform this function are not found in every dealership. It requires a very good understanding of computer networking and addresses schemes. You MUST place a good deal of trust in this person as well. Mistakes on their part can bring the dealership network completely to a halt. If service providers are not able or willing to support equipment in the dealership, an outside resource can be contracted.

4.2. ADDRESSING

An ISP should provide the dealership with routable Internet Protocol (IP) addressing. Routable addresses are required for users on the Internet to communicate with the dealership and their sites. The addresses will be assigned to the router. Devices on the Local Area Network (LAN) can use either routable addresses or reserved private addresses. OEMs recommend the use of dynamic IP addressing served by the router. If routable addresses are used, it is essential that the ISP reserve these addresses. A detailed review of IP addressing is located in the Appendix.

Network devices use a routing table to maintain knowledge about where IP networks and IP hosts are located. IP addresses and subnet masks identify these networks and hosts. In addition, routing tables are important because they provide needed information to each local host regarding how to communicate with remote networks and hosts.

Private addressing (RFC1918) uses IP addresses that have been designated for private use only. This means that these IP addresses can be used in private network environments and cannot be routed over the public Internet. Whereas non-routable addressing is IP address space that is registered with the Internet Network Information Center (InterNIC), but has not been made available to be routed over the public Internet.

4.3. ROUTING

Router configuration varies from supplier to supplier. It is best to have a professional technician handle the configuration of the router. However, there are some basic rules that installers should follow:

Change the default password. More often than not equipment manufacturers use the same default password in all of their products. These passwords are widely known. This is done so that installers can quickly get the product up and running without referring to documentation or having to call the manufacturer. If the installers change the password, make sure they give it to someone designated in the dealership as an administrator. That same person should know how to change it after the installer leaves. If the dealership is going to manage it's own router, there is no reason for anyone outside the dealership to know the password. However, at least two people in the dealership should know what that password is.

Ask for a copy of the configuration file on disk. If for some reason the router has to be replaced, having a copy of the latest configuration files on disk can save time and significant money. Rebuilding a router configuration files from the beginning can take significant time. Having a disk on hand could mean a restore time of a few minutes. Be sure to get a new copy of the configuration after each change and keep this disk in a safe place. It is also advisable to keep several generations of the configurations. Problems are not always discovered right away. It may be necessary to restore the configuration used before the last couple of changes were made in order to truly correct the problem.

Insist on labeling each interface and cable. This will save time when tracing back cables and acts as a self-documenting process others can follow.

Secure the router in a rack or on a wall shelf. Placing a delicate instrument on a tabletop or in an area where it can be moved or dropped is inviting trouble. Take the time to mount the device securely. Preferably, this should be in a rack with other communications gear.

Be sure the router can come back after a power surge. Do not let the technician leave without demonstrating that the router can restore itself after a full power outage.

The concepts of having visibility to the network and having the ability to control network infrastructure are elements that are often overlooked when installing a Local Area Network (LAN) and Wide Area Network (WAN). Consider the following requirements when purchasing a router. This will insure that the device can be serviced quickly or problems could be solved without a service call.

Management of the router via web interface, telnet or GUI software (this avoids having to go to the wiring closet to work on the router):

- Update remotely by downloading software fixes.

- Save configurations locally or remotely.
- Log all router errors.
- Conduct diagnostics remotely.

4.4. ROUTING HARDWARE

Most ISPs will offer the router as part of the service provided to the dealers. Regardless of whether the dealer chooses to purchase its own router or it is provided by the ISP, the following are some basic guidelines to follow.

Routers offer a wide range of features. Since it is a significant portion of the LAN equipment costs, it makes sense to look at models and features to determine the best fit for the dealership. The dealership will want to avoid spending too much initially. However, the ability to add features, as the dealership and the network grow, is essential. Most routers can be configured with different expansion cards and software (called feature sets) to meet the needs of the dealership.

When evaluating router technology consider the following:

- **WAN Interfaces -** Support for various Internet access methods. Although the dealership may be using an Integrated Services Digital Network (ISDN) circuit today, that does not mean it will not change to higher bandwidth technologies such as Digital Subscriber Line (DSL), Frame Relay or fractional T1 in the future. Routers should not have to be replaced if access methods are changed. Make sure that router supports multiple WAN interfaces such as Dial-up, ISDN, xDSL, V.35, T1, and Ethernet. Ethernet WAN interfaces are often needed to support the newer broadband technologies xDSL, cable, wireless, satellite, etc.
- **LAN Interfaces -** If the dealership has several separate LANs, consider a router that can support multiple Ethernet interfaces. If the dealership has to support private segments and connections to other OEMs, it may need multiple interfaces. This separation may also be done with a switch working in conjunction with the router.
- **Firewall -** Be sure that the router software includes the ability to act as a firewall with support for the following proxies: SOCKS, HTTP, HTTPS, NAT and DNS. Routers should include context-based access control for dynamic firewall filtering, denial of service detection and prevention, real-time alerts, and encryption.
- **DHCP -** If the dealership follows the OEM recommendation to have dynamic IP addressing, it will need DHCP support. Routers should act as a DHCP server. This allows addresses to be served to the internal workstations without having to employ an additional server.
- **Router Management -** Routers should be manageable via Standard Network Management Protocol (SNMP). This allows central monitoring, configuration, and diagnostics. A method of alerting remote administrators of problems is a requirement. Performance and usage information should be logged to identify usage of the network, suspected security events, and router performance. Software that allows log filtering to spot priority problems is a plus.
- **Integration -** For dealerships that want to integrate voice and data capabilities now or in the future, the ability to connect the router to telephone equipment is needed. This is usually done with expansion

cards that provide an interface to the existing telephone infrastructure including telephones, fax machines, keyed telephone and PBX system units.

4.5. NETWORK ADDRESS TRANSLATION (NAT)

Network Address Translation (NAT) is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. This allows home users and small businesses to connect their network to the Internet economically and efficiently. NAT should be a required feature in any router.

Reasons for using Network Address Translation:

- A world shortage of IP addresses.
- Concerns over security.
- Ability to use private (and therefore un-routable) IP addresses on the LAN.
- Ability to change ISPs with less disruption.

A detailed review of Network Address Translation is located in the Appendix.

4.6. DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a method of assigning IP addresses dynamically. Many routers contain the option for a DHCP server. DHCP allows client computers to be configured automatically; when a computer is switched on, it searches for a DHCP server and obtains TCP/IP setup information. Network configuration changes are done centrally at the server. The administrator does not need to apply the change to every computer in the network. The clients will be updated when the request information from the DHCP server during their boot-up cycle. For example, if it is necessary to reconfigure a private addressing scheme in order to merge the network with the network in another store, all clients will automatically start using the new addresses the next time they boot-up. Some ISPs will require the use of DHCP as a prerequisite for using their network.

4.7. DOMAIN NAME SERVICE (DNS)

The Domain Name Service (DNS) is an Internet directory service used to translate readable domain names (e.g. joes.autorepair.com) and Internet Protocol (IP) addresses (e.g. 192.168.45.230). Domain names consist of two or more levels separated by dot '.' and MUST be registered by the operator of the top level of the name (e.g. .com in joes.autorepair.com is operated by VeriSign). The directory of domain names is distributed across the Internet and DNS is widely used by most Internet services to locate Internet domains (web sites) and to control Internet email delivery. That is, a registered unique name can be entered into a browser as the identifier for a website. Computers however must still use the numeric addresses, so the text names have to be converted into numeric addresses. The Internet has a collection of

servers that together provide for two-way name-to-address translation. When Internet names and addresses are"registered" an entry is placed into the lookup tables used by DNS.

There are two types of top-level domains (TLDs), generic and country codes. The most common generic top-level domains are three letters but can be longer or shorter. The following table lists some common generic top-level domains.

Table 4.1. Common Domains

Restricted For Use By	Top Level Domain	Operated By/DNS
Commercial	.COM,.NET,.ORG	Verisign Global Registry Service (www.versign-grs.com)
Education Institutions granting four-year higher education degress in North America	.EDU	Educause (www.educause.edu/edudomain)
Organizations estrablished by internal treaty	.INT	IANA .int Domain Registry (http://www.iana.org/int-dom)
US Military	.MIL	US DoD Network Information Center (http://www.nic.mil)
US Federal Government	.GOV	US General Services Administration (http://www.nic.gov/)
Businesses	.BIZ	NeuLevel, Inc.(www.neulevel.biz/)

A standardized list of country codes domains are also used for top-level domain names (e.g. Norway is .no, United Kingdom is .uk, the United States is .us). Internet Assigned Numbers Authority (iana) at www.iana.org maintains this list.

4.7.1. How to get an IP Address and DNS Domain Name

Internet Service Providers (ISP) provides IP addresses. Operators of top-level domains provide domain names. Your ISP will associate your domain name with one or more IP addresses. Once the IP is associated to your domain name the IP is distributed through the DNS. Switching IP addresses usually takes two days.

Table 4.2. Key Factors of DNS

Advantages	Disadvantages
- A domain name is transferable to all Internet Service Providers (ISP). - More than one IP address can be associated with a domain name. - OEM communicating through a domain name does not need to take any action if the IP address	- In the unlikely event that the DNS is not operating then the translation from DNS to IP cannot happen and attempts to connect to the site by Domain Name fails until the service is available. - Initial connection to the web site is slower because the Domain Name must be mapped to the IP address through the DNS. However, once the con-

Advantages	Disadvantages
changes. The dealership can change IP address without the added coordination with the OEM. - Domain names can be used for brand name recognition purposes (e.g. yahoo.com). - Domain names typically have meaning and are easier to remember than IP addresses.	nection is made there is not difference in performance. - Switching IP addresses usually takes two days for worldwide distribution.

4.7.2. Recommendations

The OEMs recommend exclusive use of public DNS.

4.7.3. Local DNS

While use of public DNS service is recommended, you might consider your own local DNS server when:

- Support of internal and external addresses (public and private) is REQUIRED.
- There is need to resolve domain names internally.
- If DNS is needed locally either by the dealer or one of their suppliers, there must be a local DNS server in the dealership. The local DNS server must also forward requests to a public DNS.
- If two or more parties require local DNS services, it must be determined which party will act as the local DNS authority and provide the service to the dealership. This DNS authority is expected to provide a reasonable level of service and complete cooperation in the administration of DNS.
- IT resources such as servers, printers, gateways, etc. devices should be registered in the local DNS.
- hosted servers or services that have access to the Internet should be registered in the public DNS.
- Business grade DNS devices that are supported by your vendor of choice (vendors who support the device on a day-to-day basis) is recommended.

4.7.4. Compliance with Web Standards

Requests for Comments (RFCs) have been used since 1969 to build and communicate Internet standards. Committees of the Internet Society like Internet Engineering Steering Group (IESG) and the Internet Engineering Task Force (IETF) request information, review submissions, and publish standards. This process makes for open, interoperable networks and systems. All equipment, software and plans should comply with the following standards:

- RFC 791 - Internet Protocol
- RFC 1011 --Official Internet Protocols
- RFC 1055 - A Non-Standard for Transmission of IP Datagram's Over Serial Lines: SLIP
- RFC 1542 - Clarifications and Extensions for the Bootstrap Protocol

- RFC 1631 - The IP Network Address Translator (NAT)
- RFC 1661 - The Point-to-Point Protocol (PPP)
- RFC 1700 - Assigned Numbers
- RFC 1883 - Internet Protocol, Version 6 (IPv6) Specification
- RFC 1884 - IP Version 6 Addressing Architecture
- RFC 1918 - Address Allocation for Private Internets
- RFC 2068 - Hypertext Transfer Protocol â€”HTTP/1.1
- RFC 2131 - Dynamic Host Configuration Protocol Well Known Port Numbers

4.8. NON-DEALER DATA ACCESS

For dealerships' continued growth there may be need to allow Non-Dealer vendors into the network to extract information that will help generate business. This may for instance help dramatically improve sales, but if the wrong person gets in or misuses privileges the business could come to a screeching halt. Preventing people from abusing a network requires taking the proper steps for self protection.

4.8.1. Understanding the network setup

Become familiar with the following steps to avoid unauthorized users gaining access to the network:

- Understand setting up and controlling user ID's and passwords - This allows the dealer to deny access to someone that abuses or isn't allowed to be on the network. Every vendor/user that has access to the system should have a unique ID. Do not create one ID for all vendors.
- Become familiar with the network logs and peruse them regularly. This allows identification of who is accessing the system and how often.
- Suspend user IDs that exceed a threshold for unsuccessful login attempts;
- Consider using a DMZ as a secure area separate from the main systems, where only pertinent information can be made available. For more information review chapter 9.
- If feasible, apply time restrictions and hours of access for data availability;
- Understand the impact of additional traffic on the network and server, and scale or restrict resources accordingly

4.8.2. Negotiating and Auditing the contract terms

Before entering into any relationship with a vendor it is important that a detailed contract be established to ensure understanding of terms and conditions. Self protection is most important when allowing others to access dealership assets (data). There are a few key items that should be in the contract:

- The reason the supplier is accessing the system.

- What additional purposes will the data be used, if any.
- The time of the day and day of week of allowed system access.
- Specific time period of allowed system access.
- The estimated load added to the network during allowed system access.
- The vendor must guarantee to and maintain privacy all data extracted.
- The vendor must provide reports showing the date, time and duration of every system access.
- A clause that indicates remediation for failure to comply with the terms of the contract.
- How they will store and secure any collected data and how long will it be kept.

In addition to the meeting the checklist above it is important that any supplier partner have no complaints against it for bad business practices, or other negative items. Research the supplier thoroughly. It is important that a dealer be proactive when allowing anyone data access. . A trustworthy business partner should have no problem complying with reasonable expectations. It is important that a dealer be proactive when monitoring anyone accessing their data.

4.9. NETWORK SERVICES POLICY RECOMMENDATIONS

Table 4.3. Network Services Recommendations

Element	Description
Addressing	ISP should provide routable public IP addressing. Use dynamically assigned public or private addressing for devices on the LAN
Routing	Have a professional handle routing configuration. Change and protect passwords for routers. Save backup configurations to diskette. Label router and wiring properly. Mount router securely in a rack
Routing Hardware	Consider current needs and allow for future expandability when selecting routers and feature sets
Network Address Translation (NAT)	NAT should be a required feature in routers and seriously considered for connecting multiple computers to the Internet
Dynamic Host Configuration Protocol (DHCP)	DHCP should be used to simplify network configuration and administration
Domain Name Service (DNS)	The exclusive use of public DNS is recommended

4.10. USEFUL WEBSITES

http://www.corenic.org

http://www.ietf.org

Chapter 5. PRIVATE AND VIRTUAL PRIVATE NETWORKS

Table of Contents

5.1. OVERVIEW

Networks consist of connections between machines (computers) allowing the machines to communicate and work together. The simplest network is between two machines in the same room connected with a cable in that room. This network is private. It is as secure as the room occupied by the machines provided the computers do not have other connections.

When machines being connected are not in the same building, they can still be connected privately by using a connection leased from telecommunications provider. They can also be connected privately by using the public switched network. Both of these are substantially less expensive than running a private wire across a long distance.

Leased lines are expensive and the switched network is limited in communication capacity (slow). The Internet generally provides a lower-cost alternative. However, depending upon the service provider capability, these configurations may be vulnerable to third party wire taps, and messages traveling over the Internet can be intercepted by third parties with a computer and a little ingenuity. Low-end internet service providers may be more costly in the long run due to these security risks, as well as interruptions and slowdowns.

Virtual Private Networks address these concerns by providing software that makes the Internet appear as a leased connection to the machines being connected. Each machine acts as though it were connected to the other using a Local Area Network wire.

VPNs may be LAN-based or client based. Typically, LAN-based configurations use hardware to maintain the VPN whereas client-based ones require software to be installed, configured and maintained on each machine - raising the costof the VPN to greater than just using the Internet.

Privacy concerns are addressed by encrypting the message before sending it out through the VPN and decrypting on the way in. Penetrating the encryption requires a great deal of time and computing power making the VPN risks akin to the wire tap risks of leased lines.

Alternatives to VPNs could involve private networks such as ANX (Automotive Network Exchange). This network was created to allow Internet like facility between Automotive OEMs and their suppliers. ANX is not considered feasible for dealer communications because of interoperability issues and cost.

5.2. USING VIRTUAL PRIVATE NETWORKS

Private networks are closed because they limit contact with other networks. Traffic is safe and reliable because there is no possibility of interference from outside sources. There is a cost for that level of service though. Private networks tend to be more expensive because the communication medium is dedicated. The satellite networks that many of the OEMs use are examples of private networks. A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure. A VPN can use public switched networks or, in some cases, the Internet. Privacy is maintained by using software-based tunneling protocols or hardware-based gateways. A VPN can be contrasted with a system of owned or leased lines that can only be used by one company. The goal of a VPN is to give the company the same capabilities of a private network at much lower cost by using the shared public infrastructure. A VPN adds a supplemental level of security when sharing data over public resources.

Using a VPN involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. There are several ways of implementing a VPN, including client-to-server and network-to-network technologies. This extra processing requires complex network set-ups, ongoing management, and increased bandwidth requirements.

Due to the additional complexities, the cost of using a VPN is higher than that of using the public Internet even if the Internet is used to transport data. In situations where higher security is required, the cost can be justified. Where reliability is a critical factor, private networks are chosen over public options. Most of the automobile OEMs have connections to a VPN called Automotive Network Exchange (ANX). Only a few Certified Service Providers (CSP) are allowed to provide ANX connectivity service nationwide. This network handles communication among large suppliers involved in the manufacturing process. The large volume of mission-critical data transferred on this network requires the kind of dependability and safety a private network offers. Many CSP's provide Internet access through the ANX network.

ANX is not presently considered a reasonable option for dealerships to OEM communication because of interoperability issues and high costs. The kind of dependability and security needed for dealership applications can be provided using the public Internet with far less cost. Some OEM's and DMS providers may choose to use ANX or some other VPN. Those networks can also be used to communicate with OEMs that have a web presence as long as these VPNs have gateways to the Internet. Those gateways should allow individual dealers to configure Internet access and security policies.

5.2.1. Security

The most important aspect of a VPN is security. The essential elements of security are:

- **Access control** - guarantees the security of network connections.
- **Authentication** - verifies the identity of the user and the integrity of the data.
- **Encryption** - protects the privacy of the data.

5.2.2. Access Control

The VPN solution must provide access control. Once the identity of the user has been verified, the user's profile will determine exactly what services and resources can and cannot be accessed on the network. Once the authorized user is authenticated, access will be granted only to those services, applications and resources for which the user has been authorized. By providing specific application access control, corporations are now able to grant access to their most sensitive data, without compromising network security.

5.2.3. Authentication

It is very important to ensure that the users are who they say they are (user authentication) and controlling the network resources that they can access (access control). Integrated at the VPN point of access, user authentication will establish the identity of the person using the “VPN node” and eliminates the possibility of unauthorized access. A user authentication mechanism must be supplied to allow the authorized user of the VPN system access to the system, while preventing the attacker from accessing the system. Some of the common user authentication schemes are: operating system username/password, S/Key (one time) password, RADIUS authentication scheme and strong two-factor token-based scheme.

5.2.4. Encryption

Encryption is the process of making information unreadable to unauthorized users, thereby making it private. Decryption is the reverse - returning the information to its original readable form.

Symmetric - (private key, secret key, 1 key) encryption uses a secret key that is known by both communicating parties. The sending party uses the secret key as part of the mathematical operation to encrypt (or encipher) plaintext to ciphertext. The receiving party uses the same secret key to decrypt (or decipher) the ciphertext to plaintext. The distribution of the secret key MUST occur (with adequate protection) before any encrypted communication. Examples of symmetric encryption schemes are the 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), the International Data Encryption Algorithm (IDEA) and the most current Advanced Encryption Standard (AES).

Asymmetric - (public key, 2 key) encryption uses two different but mathematically related keys for each user - one is a private key known only to this one user; the other is a corresponding public key, which is accessible to anyone. The private key must be known only to the owner of the private key. In order to send a message using asymmetric encryption, the sender uses the receiver's public key to encrypt the message. The receiver in turn decrypts the message using the receiver's private key. In addition, public key encryption technologies allow digital signatures to be placed on messages. A digital signature uses the sender's private key to encrypt some portion of the message. When the message is received, the receiver uses the sender's public key to decipher the digital signature as a way to verify the sender's identity. Public key cryptosystems overcome the complexity and inherent risk involved with sharing the same key in private key cryptosystems.

The transmission mode used in the VPN solution will determine which portions of the message are encrypted. Some solutions will encrypt the entire message (IP Header and data) while others will encrypt only the data. If possible, the VPN solution should support the ability to selectively activate encryption for specific services and applications. For example, an extranet that supplies partners with product data does not necessarily need to be encrypted while access to an inventory database should be encrypted (and authenticated). Combining selective encryption activation with access control would allow a user to cre-

ate a specific encrypted session directly to the VPN application of choice, ensuring that the data was safe during transport as well as guaranteeing network security.

5.2.5. Tunneling

VPNs function using a technique called tunneling, which is essentially a process that encrypts, wraps, and sends data or information using multiple protocols from a source to a destination reliably. The concept can be roughly compared to the steps involved in sending and receiving a letter in the mail:

1. Sender writes a letter.
2. Sender seals letter in envelope (encryption, contents unreadable by casual observers).
3. Sender writes the address on the envelope (protocol used to identify receiver of letter).
4. Sender sends the letter using registered mail (Regular mail can be thought of like the Internet - no guaranteed level of service- the letter arrives when it arrives and in fact may be lost. Registered mail guarantees delivery using the same infrastructure as the regular mail, but with a guarantee. Similarly, a VPN works over the same infrastructure as the Internet and but offers a guarantee.).
5. Post office reads address on envelope and transports letter by truck, train, or plane to other post offices to receiver. (Message moves through the VPN (Internet infrastructure), using ATM, Frame Relay, DSL (truck, train, or plane) to various routers (post offices) to receiver.
6. Receiver opens letter (decryption).
7. Receiver reads letter.

5.2.6. Tunneling Protocols

A fully functional VPN solution must incorporate most, if not all, of the following protocols:

Point to Point Protocol (PPP)

RFC1661 Point-to-Point Protocol (PPP) provides router-to-router, host-to-router, and host-to-host connections over wide area links. PPP encapsulates multiple protocols including IP, IPX, AppleTalk, etc. This very basic protocol typically is used by the ISP to authenticate users.

Point to Point Tunneling Protocol (PPTP)

RFC2637 Point-to-Point Tunneling Protocol (PPTP) is a proprietary protocol from Microsoft. An extension of Point to Point Protocol (PPP) that encapsulates IP, Internetwork Packet Exchange (IPX), or NetBEUI inside IP packets, this protocol is used primarily by ISP equipment providers because it accommodates end-to-end and server-to-server tunneling. PPTP uses a TCP connection for tunnel maintenance and Generic Routing Encapsulation (GRE) encapsulated PPP frames for tunneled data. The payloads of the encapsulated PPP frames can be encrypted and/or compressed. The typical application of PPTP is to tunnel a connection from the local ISP to a corporate network.

Layer 2 Forwarding (L2F)

RFC2341 -Cisco Layer Two Forwarding (Protocol) "L2F" (L2F) is a proprietary protocol from Cisco that allows dial-up access servers to frame dial-up traffic in PPP and transmit it over WAN links to an L2F server (a router). The L2F server then unwraps the packets and forwards them into the network. The in-

formation in an L2F traffic stream is not encrypted. The typical application of L2F is to tunnel a connection from the local ISP to a corporate network.

Layer 2 Tunneling Protocol (L2TP)

RFC2661 Layer Two Tunneling Protocol "L2TP" (L2TP) is a combination of the best features of PPTP and L2F. When configured to use IP as its datagram transport, L2TP can be used as a protocol for tunneling PPP over the Internet. L2TP can also be used directly over various WAN media (such as Frame Relay) without an IP transport layer. Like L2F, the L2TP traffic stream is not encrypted. The typical application of L2TP is to tunnel a connection from the local ISP to a corporate network.

Internet Protocol Security (IPSec)

RFC2401 Security Architecture for the Internet Protocol (IPSec) is a protocol that supports the secured (encrypted) transfer of information across an IP network. IPSec defines the packet format for an IP over IP tunnel mode, generally referred to as IPSec Tunnel Mode.

IPSec Tunnel Mode uses the negotiated security method (if any) to encapsulate and encrypt entire IP packets for secure transfer across a private or public IP network. The encrypted payload is then encapsulated again with a plaintext IP header, and sent on the network for delivery to the tunnel server. Upon receipt of the this datagram, the tunnel server processes and discards the plaintext IP header and then decrypts its contents to retrieve the original payload IP packet. The payload IP packet is then processed normally and routed to its destination on the target network.

Internet Key Exchange (IKE)

IKE is a hybrid protocol, which implements Oakley and Skeme key exchanges inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.

5.2.7. Other Considerations

Traffic Management — Second component critical in implementing an effective VPN is traffic control to guarantee reliability, quality of service and high-speed performance. Internet communications can become congested, rendering them unsuitable for critical business applications unless that traffic can be prioritized and reliably delivered.

Enterprise Management — Final critical VPN component is enterprise management, which guarantees integration of VPNs into the overall security policy, centralized management from local or remote console, and scalability of the solution. Because ‘“one size fits all”’ does not apply for VPNs, the combination of these three components is required to enable practical implementation of Virtual Private Networks.

5.2.8. VPN Recommendation Guidelines

Table 5.1. VPN Recommendations

Technology/Resource	Description	Advantage
IPSec	Protocol that implements authentication and encryption	Provides confidentiality, integrity and authentication services

Technology/Resource	Description	Advantage
Tunnel Mode (IPSec)	One of two methods used to deploy IPsec	Avoids having to modify PC's, servers and enhances security
AES (128, 192, 256)	Strong encryption method	Provides strong encryption to ensure privacy
Static IP Addressing	IP address assigned by the ISP which does not change. Strongly recommended for stability of the VPN.	Simplifies administration and enhances stability and security for location-to-location VPNs.
IKE Mode	Internet Key Exchange helps implement IPsec	Enhances security and simplifies administration for VPN clients with dynamic IP addressing from their ISP
Hardware Based Encryption	Encryption processing is done by VPN devices instead of through software by VPN peers	Offers increased performance over software based methods
VPN Devices	Hardware used to create VPNs	Using hardware by the same manufacturer to get guaranteed and proven compatibility
Network Suppliers	A vendor who offers network equipment and services	Choosing a reputable network supplier who has knowledge and experience in implementing VPNs will help ensure a reliable and secure network

RFC's (please refer to www.ietf.org for the actual documents):

- 1990 The PPP Multi-link Protocol (MP)
- 1661 The Point-to-Point Protocol (PPP) (Updated by RFC2153)
- 2661 Layer Two Tunneling Protocol "L2TP"
- 2888 Secure Remote Access with L2TP
- 2341 Cisco Layer Two Forwarding (Protocol)
- 1701 Generic Routing Encapsulation (GRE)
- 2637 Point-to-Point Tunneling Protocol

IPSec RFCs:

- 2401 Security Architecture for the Internet Protocol
- 2402 IP Authentication Header
- 2406 IP Encapsulating Security Payload (ESP)

Check the encryption regulations of the country where the dealership resides.

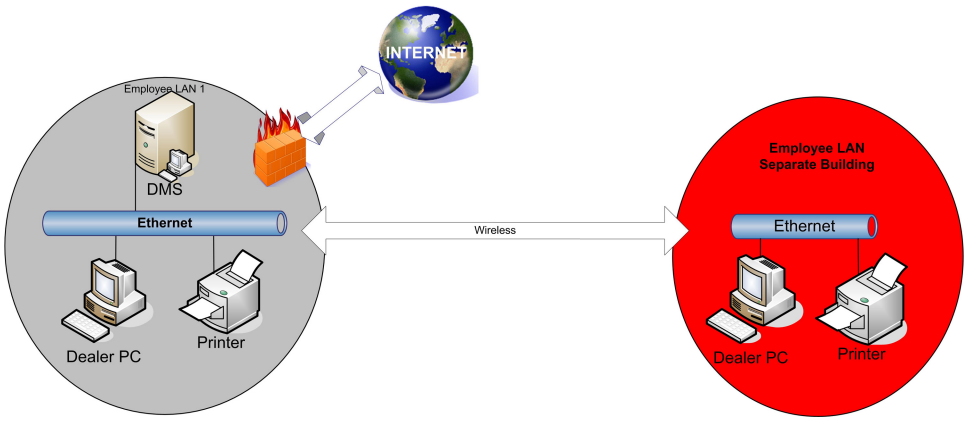
Chapter 6. WIRELESS NETWORKS

Table of Contents

6.1. OVERVIEW

Wireless LANs enable network communication and connectivity without the physical restraints of hard wired cabling. (see Figure 6.1, “Wireless LAN”). Wireless technology can be especially useful in building-to-building communication or connecting laptops, printers, or other wireless capable items such as PDAs to a network where wired cabling is difficult or expensive. Gaining a better understanding of wireless technologies (types, protocols, leading trends, etc) will be an important foundation to begin researching and exploring how wireless networks can fit your needs. Keep in mind that wireless technology and protocols are constantly changing which will require the person to stay up-to-date and informed on the latest information.

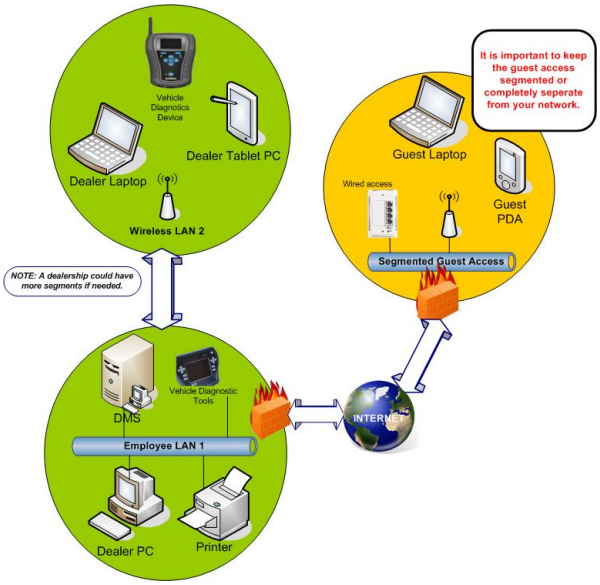
Figure 6.1. Wireless LAN



There are many situations where a wireless solution can be very beneficial. Users can now move freely from office to office, building-to-building, and location-to-location and access network resources and the

Internet. A wireless network can be leveraged for a temporary set up during remodeling, peak seasons, or special projects such as tent sales. If the dealership is utilizing wireless for the primary means of network connectivity it is important to ensure redundancy in case of outages and full bandwidth for full coverage and connectivity.

Figure 6.2. Access Point



6.2. COMPARISON OF 802.11G, N AND A

Currently the primary standard used in the deployment of wireless communications, is 802.11n and is recommended for new installations. However, where frequency interference has been identified as an issue 802.11a or 802.11g may be a solution. Comparisons of these are documented below.

Table 6.1. Comparison of wireless communications

Description	**802.11n**	**802.11a**	**802.11g**
Approved Date	Est June 2010	2001	2003
Frequency Band	2.4GHz	5.0 GHz	2.4GHz
Speed	100-200Mbps	Up to 54 Mbps*	Up to 54 Mbps
Estimated 128Mbps	Estimated 128Mbps	27 Mbps	20-25 Mbps
Range 1	230ft range	60 ft range	100 ft range
Modulation Technique	multiple-input multiple-output (MIMO) and Channel-bonding/40 MHz	Orthogonal Frequency Division Multiplexing (OFDM)	Spread Spectrum (DSSS/ PBCC)
Interference Issues		Less interference than 802.11b or g	Increased interference (portable phones, microwaves, ovens, etc.)

Description	802.11n	802.11a	802.11g
Product Maturity	Official Specification to be finalized in June 2010		Official specification finalized in June 2003
Distance Between Access Points		Approx. every 50 ft	Depends on configuration
Biggest Advantage	Highest speed and range	Higher speed	Higher speed coupled with 802.11b compatibility

6.3. WIRELESS RECOMMENDATIONS

The General recommendation is the industry standard wireless LAN 802.11g for new installations, which uses unlicensed radio frequencies in the 2.4GHz band without requiring line of sight for most installations and offers the highest speed and greatest distance combination. Please refer to Wireless Recommendations for important information, requirements and recommendations on incorporating security to any wireless network.

Use 802.11n only when:

- The business desires higher speeds and range and is comfortable with less mature technology.

Use 802.11a only when:

- There is significant RF interference present in the 2.4 GHz bandwidth and the 802.11g wireless network is not feasible.

Use 802.11g when:

- You wish to implement a new wireless network or there is already an 802.11b wireless network in place and backward compatibility MUST be maintained.

6.3.1. Implementation Guidelines

A qualified supplier should be able to provide assistance in making an accurate estimate of business needs. It is recommended that credentials, certifications and references be obtained.

Site Survey and Planning (Typically performed by wireless vendor)

- Check for interference caused by existing wireless LANs, Bluetooth devices, telephone systems, etc. This interference will degrade performance and in some instances may stop LAN or telephone activity.

- Ensure the site survey is performed by a wireless integrator or similar vendor using a radiation pattern detection device.

- Identify areas to be avoided with other electromagnetic interference (EMI) devices or arc welders.

- When using a wireless ISP connection, make sure that does not interfere with the wireless LAN or vice versa.

- Wireless networks should be on a separate Ethernet segment to provide broadcast isolation from rest of the network to optimize performance.
- Each access point needs to be powered. Utilization of power over Ethernet is recommended. See the glossary for more information.
- Devices should be easily upgradeable.

Installation

- Verify performance (bandwidth, retransmissions, etc.) after installation and obtain a hard copy report.
- Wireless technology is a shared media (unlike a switched Ethernet) and as devices are added to each access point, the bandwidth per device will decrease.

Security

- The OEMs recommend access points and Network Interface Cards (NICs) that are detailed in the Wireless LAN Security section.
- Hardware based encryption provides performance advantages.
- Password authentication should be used to increase security.
- The OEMs do not recommend the use of wireless LANs with applications that require large file transfers (e.g. Server backups, or Large Image files). Use in areas with other EMI devices or arc welders should be avoided.

6.4. WIRELESS LAN SECURITY

The need for security on any network is paramount, even more so with wireless networks. Typical wired networks have a degree of security inherent in them because physical access is limited by the confines of a building structure. Wireless networks on the other hand are more vulnerable because data is transmitted through the air, making access possible from anyone within range of the wireless access point.

A comprehensive wireless security solution can protect interests and thwart attacks. Proper security implementation is essential, as someone with a laptop or handheld device with wireless LAN capabilities sitting in the parking lot or across the street can access the network. Anyone with access to the Wireless Local Area Network (WLAN) can launch Internet attacks, or more concerning, may eavesdrop on network traffic. This exposes user information.

Anyone successful in obtaining user account information can gain access to databases, steal sensitive customer information, and install back doors via modems and the Internet. Malicious hackers may even destroy data, halting or severely hampering business operations. Wireless handheld devices and neighboring businesses with improperly configured WLANs within range can inadvertently access each other's networks causing performance problems. A comprehensive security solution can be achieved by using

- Encryption
- Authentication

- Firewalls
- Media Access Controller (MAC) address filtering
- Changing the default settings

All of these measures are integral to a comprehensive security policy, which is only as strong as its weakest link. Planning and implementing wireless network security has significant costs associated with it. In most cases the cost of having a strong security model clearly out weighs that of having information stolen or corrupted. A clear cost benefit should be established before choosing wireless solution over wired traditional methods. Careful planning should be exercised to ensure that the WLAN is as secure and cost effective as traditional wired methods. Consulting with a professional wireless LAN expert should be considered when planning a wireless LAN.

6.5. WIRELESS SECURITY OPTIONS

There are several different options when it comes to wireless security. The two main formats are WPA and WEP. Previously WEP was the industry standard; however with new technologies and stronger requirements a new standard has emerged. WPA is a stronger and more effective format. It is strongly recommended that all security settings be update to utilize the new standard. Note: some legacy devices may not be able to update to WPA or WEP.

Because security is ever changing and more robust tools are introduce to combat hackers it is important that a dealership be diligent with staying informed of new technologies to help protect vital infrastructure and data.

6.5.1. Wi-Fi Protected Access (WPA)

WPA is the new standard for wireless security. It secures many of the significant holes that are in the Wired Equivalent Privacy (WEP) standard where programs like AirSnort and WEPcrack were used to capture data and generate the WEP code. Although WEP is still a viable option for the home network, WPA should really be used for the business environment.

WPA is a subset of the 802.11i standard. It is also expected to maintain forward compatibility with the specification. It changes the length of the initialization vector (IV) for encrypting data to 48 bits which expands the possibilities to over 500 trillion possible combinations. It also integrates Message Integrity Code (MIC) which has built in counter measure components. The final integration point is using Temporal Key Integrity Protocol (TKIP) which works to generate pre-packet keys. All these new security features help to make WPA the choice for secure networks.

WPA (now WPA2) runs in two modes: Enterprise or Personal mode. Enterprise requires an authentication server and uses RADIUS protocols for authentication and key distribution which centralizes the user credentials. This setup takes more time to complete and a higher skill set, but offers the most secure installation.

The standard length of the initialization vector for encrypting data The Personal or Pre-Shared Key or K (PSK) mode operates much the way that the existing WEP implementation works. It used a â€œShared Secretâ€ key to generate the encryption packet. Where it differs from WEP is the added security that is mentioned above with the 48 bit IV code, the MIC, and the TKIP implementation. The biggest security concern with this implementation is that if the "Shared Secret" is compromised, the network admin has to

physically touch each wireless network node (access points, client PCs, etc.) to change the secret. It is also important to note that 802.11n requires WPA not WEP.

6.5.2. Wired Equivalent Privacy (WEP)

WEP is the popular standard for WLAN security. However this is now the legacy version of security. Most wired LANs do not use encryption to prevent eavesdropping. It is assumed that controlling physical access alone is prevention enough. WEP was developed to make 802.11b WLANs equally as secure as wired LANs by using 40-bit or 128-bit encryption methods to prevent eavesdropping. The OEMs recommend that WEP alone is not secure enough for protecting a dealership's private network.

Some 802.11b WLAN vendors are addressing the problems with WEP by enhancing their products to offer some additional security features. Devices that issue keys dynamically instead of statically have less risk of those keys being recovered by an attacker. Two-way authentication between wireless devices provides additional protection from certain attacks as well. These features offer a work-around to shortcomings of WEP; however they will not inter-operate with devices from different vendors.

User authentication is a core component of any network security solution. Authentication will prevent unauthorized access to valuable data and resources. The solution is two fold. First, requiring a user name and password in order to gain access to the LAN itself and second, to require a user name and password to log on to resources such as servers, applications and Internet access. User authentication is critical, without it networks and data are extremely vulnerable.

6.5.3. VPN

Virtual Private Networking (VPN) and data encryption technology, such as the secure sockets layer, offer an alternative to WEP. Steps should be taken to protect data from eavesdropping. This can be achieved by encrypting the data before it is transmitted and decrypting the data after it arrives to the user. The exchange of electronic keys allows the encryption and decryption to take place. When the user tries to access the network he will be issued a key, this key enables the user to read the data when he receives it. If another party intercepts the data he will not be able to read it because he does not have the key that was issued to the legitimate user.

VPNs provide protection against eavesdropping by using encryption and allow access from trusted entities exclusively. A VPN device installed behind the access point will allow users to create secure connections via software loaded on wireless workstations (client VPN). Secure building-to-building connectivity can be achieved by installing VPN devices behind access points in both buildings (gateway to gateway VPN). VPNs are typically used to provide remote LAN access via the Internet. Some parallels exist between Internet VPNs and Wireless VPNs. See Private and Virtual Private Networks for more information.

6.5.4. SSL

Likewise, the secure socket layer (SSL) is typically used to encrypt data transferred between a secure Internet website and a browser on a client device. Some website URLs will transition from "http" to "https" (as indicated by browsers in the address window) or the browser will show a padlock symbol once SSL is encrypting the data. The beauty of either the SSL or TLS is their simplicity for the client device most, if not all, browsers have it built-in without the need for software to be loaded. The real challenge for using the SSL resides on the server side which needs to supply a digital certificate authenticated by a Certification Authority and encrypt interactions with usually more than one client device. Of course, not

all computer-to-computer interactions are browser-based, so the SSL has been incorporated in other applications as their economics permit.

6.5.5. Dealership-Private Wireless LAN Recommendations

There are many steps that can be taken to avoid the possibility of access to the network from an unauthorized individual or device. While there are no procedures that will completely safeguard any network from unauthorized access, abiding by these recommendations whenever a wireless network is in place in a dealership reduces the ability of an unauthorized person to access, steal or otherwise corrupt data.

Implementing the minimum security measures stops the average person driving or walking by from attempting to get into a network, but it does not stop a skilled hacker who wants to get into your network. To stop this type of attack, additional security measures are needed, and these are documented below as well.

The minimum and additional recommendations are broken into two categories, the first one for legacy private wireless LANs and the second one for new private wireless LANs. The recommendations for legacy WLANs should be considered interim solutions and phased out in preference of the recommendations for new WLANs as new hardware is added and older equipment is replaced. Some older equipment may have firmware updates available allowing it to support WPA of new WLANs. Older or legacy equipment that does not support at least WPA and cannot be updated should be replaced altogether.

It is also recommended that on either LAN the dealership segment any guest user access completely from the main network or create a separate connection. It is also important to utilize the minimum safety measures of a firewall or MAC addressing.

Table 6.2. Minimum Recommendations for Private Wireless LANs

Legacy Wireless LAN	
	- 128-bit WEP (Wired Equivalent Privacy) key must be enabled
	- Enable MAC (Media Access Control) filtering into each access point
	- Change the WEP key and MAC filtering whenever an authorized user becomes unauthorized
	- Turn off SSID broadcasting
	- Change the manufacturer's default SSID to unique ID on the access point
	- Enable user authentication for the access point management interface, i.e. change the manufacturer's default usernames and passwords
	- Occasionally check for rogue (or unauthorized) wireless access points, for channel conflicts, and for client devices that permit ad hoc wireless connections
	- Turn off ad hoc wireless connections
New Wireless LAN -Contract with a qualified wireless vendor for recommendations	

Legacy Wireless LAN	
	- Same last 5 recommendations listed above for Legacy WLAN
	- Change the WPA key whenever an authorized user becomes unauthorized
	- WPA should be used whenever possible. This could include one of two methods:
	1 - Enterprise - Uses a server and needs more administration
	2 - Pre-Shared Key - easier to set up, but still covers the security holes in WEP

As noted in the previous section, configuring the wireless network to the requirements listed above should stop the transient person attempting to get into a wireless network fairly easily; it will not keep a person with the proper tools who wants to get into your network. While no set of security measures is ever fool-proof, the following recommendations should stop even the most serious hacker.

Table 6.3. Additional Recommendations for Private Wireless

Legacy Wireless LAN	
	- Create a VPN tunnel by installing a VPN client on each client device and configuring the VPN device, which is placed behind the access point. Note: not all VPN client software is compatible and/or interoperable with other VPN products. Consult a qualified professional before installing any VPN client software.
	- Configure the firewall, which is placed between the access point and the wired LAN, to allow only VPN traffic and deny all other traffic
	- Install a server-based user authentication system, which requires a user name and password for any device to access the network as well as applications, servers, etc and confirms it with a secure user directory
	- Attach access point to a VLAN capable switch â€“ allows for multiple VLANs to be defined for specific user groups and OEMs
	- Install uni-directional vs. omni-directional antenna where appropriate
	- Automatically detect and report rogue wireless access points and client devices that permit ad hoc wireless connections
New Wireless LAN - Contract with a qualified wireless vendor for recommendations	
	- Same last 4 recommendations listed above for Legacy WLAN
	- IEEE802.11i or WPA2 in Enterprise mode

6.5.6. Guest Wireless LAN Recommendations

Network access for guest use can be made available via wireless connectivity. However it is important that the dealership keep the guest access separate from the main network. This can be accomplished through segmenting or through a completely separate connection. See figure 5.2.1-2 Access Point. The

security recommendations for wireless guest access do not need to be nearly as protective as they need to be for a dealership's private wireless LAN there is much less at stake plus guests should be accustomed to accepting and guarding against the risks of connecting to a public network.

The overall goal of a guest WLAN is guest satisfaction at a cost justifiable for the dealership. Therefore, the guest WLAN, unlike the dealership private WLAN, should be devised to make it easy for guests to gain access without excessive dealership cost. The complexities associated with MAC filtering and WEP or WPA tend to discourage guest use and will unreasonably increase administrative overhead for the dealership. As discussed earlier, wireless simplicity tends to increase security risks. For instance, the lack of WEP or WPA makes a guest wireless LAN susceptible to man-in-the-middle attacks and eavesdropping. If guests do not use VPNs, secure sockets, or some other form of end-to-end encryption, they are vulnerable to disclosing private information to unauthorized parties who intercept their wireless communications. Not preventing the use of ad hoc WLANs or wireless connections directly between guest computing devices also increases security risks. Guest computers may still be configured with their in-home or in-office settings to share built-in data storage devices with connecting devices; therefore, ad hoc WLAN connections would permit unauthorized access to private information. Implementing the minimum recommendations shown below for a guest WLAN should provide the same levels of administrative overhead and guest satisfaction common to the retail industry.

Minimum Recommendations for Guest Wireless LANs:

- Separate the guest network from the dealership's private network.
- Post a Terms of Use statement in guest areas and present it as the first webpage accessed by guests.
- Adjust wireless access point signal strength to restrict it from unauthorized areas, e.g. across the street.
- Activate SSID broadcasting.
- Change the manufacturer's default SSID to a unique ID on the access point.
- Enable user authentication for the access point management interface, i.e. change the default username and password.
- Occasionally check for rogue (or unauthorized) wireless access points and for channel conflicts.

Chapter 7. DEALERSHIP SECURITY

Table of Contents

7.1. OVERVIEW

The most important element of a good network design is also the most often overlooked – security. Too often security outlays are considered expensive, never ending line items that can be trimmed or eliminated when looking for budget reductions. However, security spending is a strategic investment that protects the business. There is no single magic ingredient to the formula for complete network security. Some networks simply place a firewall device between themselves and the Internet and assume that all is safe. In reality, even the best firewall provides minimal help if its configuration is weak or out of date. A proactive security approach will help avoid problems by layering people, hardware, and software to create reasonable and safe protections around the network.

7.1.1. System Administration

A good security plan starts with good system administration. This role does not have to be embodied within a single person whose sole job is to administer to dealership hardware and software needs. Duties can be part time, shared, or even outsourced. However, it is paramount that the dealership has personnel that understand how the network and computer systems operate, what software is used and why, and how that software and hardware is configured. That knowledge is required to develop configurations that lock down the unnecessary system privileges that are taken advantage of by attackers. System administrators should receive ongoing training to stay up to date with recent security bugs and attacks. Most importantly, they need the unrestricted support from management in their pursuit of a secure system.

7.1.2. Physical Security

Most security breaches occur because of poor physical security. Far more breaches occur when internal users gain access to data for which they have not been granted privileges than when external hackers or spies gain access to the system. Passwords that are not kept secret or are easy to guess, “spare” user accounts that are rarely used and workstations in public areas that are not password protected, all allow for easy access into the network. User and password administration should be restricted to only a few people in the dealership, and those people should follow documented procedures to establish users, set passwords, and grant privileges. An easy method to bypass security barriers is to use a modem that is connected to a networked Personal Computer (PC). Modems should only be connected to devices used for remote support and Internet access backup with appropriate security measures in place. All PC’s connected to the Local Area Network (LAN) should have their modems disconnected. If they must be used, they should only be used for making outgoing calls. Auto-answer should be disabled whenever possible. Modems that are configured to answer calls automatically are a security threat. Hackers using tools that detect the presence of modems may discover them and use them to access or destroy dealership data.

7.1.3. Network Monitoring

Monitoring network access is another important ingredient. Network attacks rarely work the first time. All of the servers and security hardware should log any attempts to connect to them. Those logs should be reviewed daily to look for signs of possible attacks. Firewalls often generate these reports automatically. Software to compress and summarize those logs is also available. Logs can also be used to better understand the workings of the network and to help anticipate the need for system upgrades well in advance. **Comparing network monitoring systems and intrusion detection systems can also assist in the overall analysis of dealership security.** *A key here is for the administrator to trust their instinct. If something does not look right, act on it. It is easy to act after an attack succeeds, but, of course, it is too late*.

7.1.4. Software Configuration

Every device on the network should have its software configuration scrutinized for potential problems. Unused and unneeded software should be removed from systems. Access to servers should be restricted to only those ports that known software packages require. Remote control software that allows external users to run internal machines, usually over a modem, should not be permitted. Websites dedicated to systems security and administration are available that will help identify known security problems with software packages. If any of these packages are in use on the network, fixes should be downloaded and applied.

Most security plans begin with software tools or hardware devices. However, it is the thoroughness of the policies and procedures of the previous four elements (systems administration, physical security, network monitoring, and software configuration) that allow for the success of these tools. Only if access is funneled through expected gateways on known paths can intrusion detection software and firewalls offer complete protection. Costs for these devices can range from nothing to six figures. However, increased cost does not always buy increased security. If the knowledge of the network software and hardware is complete enough, firewall software running on the Internet router can provide excellent protection. Do not overlook the need to scan email and hardware for viruses. Very high-profile attacks have occurred recently in the form of email attachments. Anti-virus software is essential to avoiding those kinds of attacks.

7.1.5. Quality Assurance

Finally, hackers are moving targets that constantly search for new ways to exploit networks. The final element to any good security plan should include frequent reviews and audits to insure that known holes are plugged. Attempts should be made to break into the dealership's own network. Dial all telephone numbers to see if an unexpected modem answers. Consider the use of outside auditors on a regular basis (at least yearly). Many consulting firms and CPA's now offer these kinds of audits. An audit MUST test every aspect of network security. Firewalls, mail, Domain Name Server (DNS), domain, web, and File Transfer Protocol (FTP) servers should all be evaluated.

On the surface, these precautions may seem overly detailed. Security professionals are often accused of crying wolf. Nevertheless, the cost to recover from even one attack can easily pay for all of these efforts. Attacks are becoming more frequent as is evident by recent reports in the media. The story being told by the media is that thousands of people and businesses are being hurt by the attacks. What they are not reporting on is the tens of thousands that were not hurt because they had tight, secure network plans and they took immediate action when a threat was discovered.

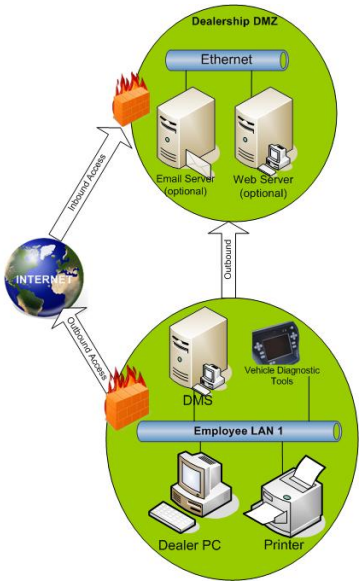
7.2. FIREWALLS

A firewall examines all traffic attempting to pass between two networks and only passes traffic that meets predefined criteria. The firewall should be placed so that all inbound and outbound Internet traffic MUST pass through it. No backdoors or other network paths should be available. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network, and trigger alarms when hostile or unauthorized entry is attempted.

Does every dealership need a firewall? Yes! Any private LAN network that is connected to the Internet needs firewall protection. Furthermore, anyone who connects so much as a single computer to the Internet via modem should have at least personal firewall software. Many dial-up Internet users believe that anonymity will protect them, feeling that no malicious intruder would be motivated to break into their computer. Dial up users who have been victims of malicious attacks and who have lost entire days of work, perhaps having to reinstall their operating system, know that this is not true. Irresponsible pranksters can use automated robots to scan random IP addresses and attack whenever the opportunity presents itself.

Firewalls should run on network appliances, such as routers, or UNIX servers. Operating systems such as Microsoft Windows should not be considered to host firewall software due to security risks.

Figure 7.1. Dealership Demilitarized Zones (DMZ)



Blocking vulnerable ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. Even after these ports are blocked, they still should be actively monitored to detect intrusion attempts. WARNING: Blocking some of the ports in the following list may disable needed services. During the initial configuration, all Transmission Control Protocol (TCP) ports should be disabled. Ports should then be enabled only for identified applications. Standard ports should be used whenever possible. Please consider the potential effects of the following recommendations before implementing them (although this list represents many of the known potential problems, understand that it is not inclusive):

- Block “spoofed” addresses — packets coming from outside the dealership sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source-routed packets.
- Log-in services— telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al. (512/tcp through 514/tcp)
- RPC and NFS— Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
- NetBIOS in Windows NT — 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 – earlier ports plus 445 (tcp and udp)
- X Windows — 6000/tcp through 6255/tcp
- Naming services— DNS (53/udp) to all machines that are not DNS servers, DNS zone transfers (53/tcp) except from external secondary, LDAP (389/tcp and 389/udp)
- Mail— SMTP (25/tcp) to all machines that are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
- Web— HTTP (80/tcp) and SSL (443/tcp) except to external web servers; may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)

- “Small Services”— ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)

- Miscellaneous— TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

- ICMP— block incoming echo requests (ping and Windows trace route), block outgoing echo replies, “time exceeded” and “destination unreachable” messages except “packet too big” messages (type 3, code 4). (This item assumes that the dealership is willing to forego the legitimate uses of ICMP echo request in order to block some known malicious uses.)

To further lock down your Internet connection, certain inbound access methods can be used. The following examples of inbound access will discuss the positives and negatives of each method. The positive:

7.2.1. Inbound Access Examples

Highest level of security - Blocking all inbound access (Only Virtual Private Network (VPN) (Please refer to chapter 8) or DMZ activity) – Only traffic originating from within the dealership is allowed out and back in.

Positive

- Provides highest level of security – no inbound traffic means that the dealership can spend more time looking at the traffic that originating from within the dealership and not as much on the incoming traffic. This by no means that the dealership can take a “hands off” approach to the problem, but that in the scope of security, this solution give the best protection in an ever changing world.

- Easy to implement – Most firewalls come standard with no inbound access. It has to be specifically allowed for inbound access. Check with your firewall vendor before this is assumed.

Negative

- Very restrictive – Some applications may not work with this method. Other methods will need to be used (i.e. DMZ, VPN, etc.) to allow applications to work which require a high level of knowledge to implement.

Middle level of security - Allowing IP to IP inbound access – this method uses a source and destination IP address for communication and usually has a port access list associated with it. Positive.

- Middle level of security – this method uses a source and destination IP so the communication to the dealership can be fairly confident who is sending and receiving the traffic. Also ports can be specified to further lock down the security.

Negative

- Less restrictive – Applications can now work through the internet. The dealership needs to be concerned with attacks like

- Harder to implement – A working knowledge of Internet Protocol (IP), Ports, and firewalls is needed to set this up.

- Dealership needs to be aware of security vulnerabilities with this infrastructure
- “Man in the Middle” where a malicious user will highjack the IP of the source and destination. This attack is used to collect a copy of the information that is being transferred. Authentication (i.e. certificates) can be introduced to solve this problem, but this requires a higher level skill set to implement this technology.
- Spoofing is the creation of Transmission Control Protocol / Internet Protocol (TCP/IP) packets using somebody else's IP address. Routers use the "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. That address is only used by the destination machine when it responds back to the source.
- There are many more attacks to be cognizant of. It is up to the network manager to constantly keep up to date with these attacks.
- More Maintenance
- Static vs. dynamic IP
- Remote users (VPN, Secure Sockets Layer (SSL)
- Authentication policy

Lowest Level of security - Opening ports to the inside network – this method opens a port (such as port 80 “www”) to a machine on the inside network. Positive

- Non restrictive – Web servers and application are easy to access and takes very little administration.

Negative

- Low level of security – This method opens up a port to a particular port on the dealership’s network (i.e. Mail Server, Web server). This method allows ANY user on the Internet to access this machine through this port. If this machine is compromised, then the malicious user could have access to the rest of the dealership’s network.
- Harder to implement – A working knowledge of IP, Ports, and firewalls is needed to set this up.
- No Firewall – In this Internet age, it is without question that a firewall is a MUST to protect the data of the dealership as well as the information of the customer. The STAR organization does not support this approach.

Summary – All the items that have been discussed are solutions that work, however, STAR is moving towards eliminating the lower and middle security methods. With many providers selling and implementing solutions, a dealership MUST do everything possible to protect its network the information contained within it.

7.3. PACKET FILTERS

Packet filters deliver the most basic form of firewall security and are a standard feature of most routers. Although packet filtering should always be used, it only provides minimal protection and MUST be used

in conjunction with other firewall techniques. Packet filters inspect the header of each incoming and outgoing packet for user-defined content, such as an IP address or a specific bit pattern, but do not validate or track the state of sessions. Packet filters can also filter at the application port level (e.g., FTP generally uses port 21). However, since any packet with the right IP address can pass through the filter once the port is enabled; there is a security hole for other applications or sessions addressed to the same port.

Source routing is a routing mechanism whereby the path to a target machine is determined by the source, rather than by intermediate routers. Source routing is used mostly for debugging network problems but could also be used to attack a host. If an attacker has knowledge of some trust relationship between hosts, source routing can be used to make it appear that the malicious packets are coming from a trusted host. Therefore, because of this security threat, a packet filtering router can be configured to reject packets containing source-route options. Thus, a site that wishes to avoid the problem of source routing entirely would write a policy to that effect.

Packet filters can be used in a variety of ways to block connections to or from specific systems or networks, and to block connections to specific ports. A site might wish to block connections from certain addresses, such as from systems or sites that it considers hostile or untrustworthy. Alternatively, a site may wish to block connections from all addresses external to the site (with certain exceptions, such as with Simple Mail Transfer Protocol [SMTP] for receiving email).

7.4. PERSONAL FIREWALL SOFTWARE

Personal Firewall Software operates like a persistent “traffic cop.” When the Personal Firewall Software detects inappropriate access to a computer, it blocks access to the offending user. Other Internet access remains open and unaffected. The user can continue to browse the web, send email, and listen to Internet radio stations while Personal Firewall Software rejects the hackers.

When a Personal Computer (PC) connects to the Internet, it becomes part of a global network. A hacker can use widely available networking tools to connect to that computer and send it commands. Since the link to the Internet is active hackers can identify the user’s system and break into it.

The Personal Firewall Software should consist of two components:

- The detection and protection mechanism that guards a computer from attacks and the summary application, which provides a user-interface to the Personal Firewall Software.
- Together these components should provide the same level of security as the firewall software in the router.

Personal firewalls have a place on every machine, but there are areas where they become a necessity. Traveling personnel with portable devices should always use a personal firewall since there are no guarantees that the network that they are on has a firewall. Understand the placement of firewalls on every machine can add additional administrator overhead since it takes someone to look at all the policies to determine what is actually correct to block and what should not be.

Corporate networks can also benefit from using personal firewalls. Most attacks come from internal malicious users, so a firewall on every laptop, PC and server can help with this kind of attack. Also, since most personal firewalls can monitor outgoing traffic from the PC, it is easier to identify and attack security vulnerabilities like Trojans and worms.

7.5. DEMILITARIZED ZONE

If connections inbound from the Internet are required, the dealer should set up an external safe area usually called a Demilitarized Zone (DMZ or Transaction Zone). A DMZ is a portion of the network that logically sits between the Internet and the local area network (see Figure 7.1, “Dealership Demilitarized Zones (DMZ)”). Physically, a DMZ is established as a separate segment with traffic directed to it from the dealership router. A DMZ is accessible from both the internal network and the Internet, but does not allow machines on the Internet to access directly the dealer’s internal network.

This DMZ configuration creates a divided approach. Information that is bound for the internal network now has to make twp stops (one into the DMZ from the Internet and one from the DMZ to the internal network). Users who are sending this content do not have direct access to the internal network. This is important as the network administrator can stop any traffic at any time for certain applications if he/she feels there may be a malicious attack.

The normal install of A DMZ configuration consists of firewall rules governing access to servers inside the DMZ and another set of rules governing access to and from the internal network in order to enable them to perform specific functions. It is important to make these rules very specific down to IP and port number. It is even more effective if the rules are set up in such a way that internal machines are the only machines that can initiate a conversation with the DMZ, versus a DMZ machine that can access the internal network. With this configuration, a compromised (or hacked) machine on the DMZ is still very limited to what it can do and only has access to the DMZ it sits on.

Servers used to host dealership websites and external email services MUST be placed within the DMZ. Dealerships that allow inbound access to their networks should be aware that there is a broader scope of issues that exist which are not covered in this document. Dealerships should have a highly qualified supplier configure and maintain these networks.

7.6. PROXY SERVER

Proxy servers provide additional security by hiding networks from each other. All communication between the networks goes through the proxy. In a dealership environment, the PC’s communicate with the proxy server, and the proxy server in turn communicates with the Internet. Data packets going to the Internet are “repackaged” with the IP address of the proxy server, so that intruders are not able to determine the true source of the packets.

A proxy server has many potential purposes, including:*

- **To speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server.**
- **To apply access policy to network services or content, e.g. to block undesired sites.**
- **To log / audit usage, i.e. to provide company employee Internet usage reporting.**
- **To bypass security/ parental controls.**
- **To scan transmitted content for malware before delivery.**

- **To scan outbound content, e.g., for data leak protection.**

Proxy servers are not required to communicate with the OEMs over the Internet. However, they can be configured to provide additional services that may be desirable. These services may include:

- **Authentication** — the process of identifying and verifying any individual attempting to gain access to a network.
- **Authorization** — the process of determining whether an individual has the right or authority to perform an operation on a protected resource. Authorization services are a critical part of an application's security architecture. After a user authenticates his identity, authorization services enforce the business policy by defining what services and information the user can access.
- **Caching** — the storage of recently accessed web pages for quicker retrieval.
- **Logging** — the automatic generation and storage of service requests including those who access to the Internet.
- **URL filtering** — the ability to prevent users from visiting undesirable websites.

7.7. INTRUSION DETECTION AND PREVENTION SOFTWARE

Intrusion Detection Software (IDS) is used to provide an indication of a potential or real attack. It does not stop any attack. An attack or intrusion is a transient event, whereas vulnerability represents an exposure, which carries the potential for an attack or intrusion. The difference between an attack and vulnerability, then, is that an attack exists at a particular time, while vulnerability exists independently of the time of observation.

An intrusion detection system examines system or network activity to find possible intrusions or attacks. Intrusion detection systems are either network based or host based; suppliers are only beginning to integrate the two technologies.

Network based intrusion detection systems are most common, and examine passing network traffic for signs of intrusion. Host-based systems look at user and process activity on the local machine for signs of intrusion.

Intrusion Prevention Software (IPS), which is the next generation of IDS, works more in a real-time environment to identify and STOP attacks. IDS identifies the attacks and notifies the network administrator where as IPS actually tries to stop the attack.

IPS works under the same framework that IDS works, so network or host based clients still apply. The biggest difference is that a network administrator will get a warning that an attack has been stopped versus searching logs and trying to determine if an attack has happened.

7.8. ANTI-VIRUS PROTECTION

It has been estimated that Melissa, the ExploreZip.worm and other such malicious virus attacks cost U.S. businesses in the late 1990's a total of 7.6 billion dollars (U.S.) during a 12-month period. With

the serious potential for that kind of damage, it seems imperative that all efforts be taken to protect the dealership's network and information. Protecting networks from the growing threat of these costly computer viruses is no simple task. Over 45,000 viruses are known today and new ones are being created each month. With that in mind, fail-safe data protection is crucial. The effort begins with proper tools and continues by keeping ever vigilant for new viruses and by updating the tools used to combat them. Viruses can invade the system in a variety of ways. Files copied from infected diskettes, Trojan Horses acting as email attachments, or worms placed on servers by hackers can all wreak havoc if left unchecked. For those reasons tools are required at all levels of the network to protect the network investment and the information assets completely.

7.8.1. Client Protection

Client protection requires that software be loaded on desktop units to scan the hard drives and memory for problems on that individual machine. Scans should be scheduled to run automatically at regular intervals. Workstations with extremely important data should scan for viruses whenever they are powered up or rebooted. Software should provide for virus detection and removal. Aggressive use of desktop software will reduce the chances of harm to an individual workstation and can eliminate a virus before it infects multiple workstations. Key features include automatic update. With this feature, the software will use the Internet connection to go the website of the software maker and download any new updates. This makes it possible to detect new viruses as soon as the software maker has an update available. It also keeps all workstations up to date without anyone having to manually load new code.

7.8.2. Firewalls, Routers and Server Protection

Software on firewalls, routers, and servers MUST:

- Scan all Internet traffic, email, and file attachments.
- Remove viruses before they invade the computer network, and repair damaged files.
- Anti-virus software should scan the memory and hard drive of both servers and clients.

Tools MUST be able to handle common compressed-file formats. Virus writers often target compressed files as another place to conceal new viruses. As today's viruses transmitted via email are notoriously fast spreading, it is essential that companies use an anti-virus solution that includes mechanisms to assure the quick application of a cure. Software should:

- Scan and deliver all clean traffic.
- Immunize or destroy known viruses and quarantine anything else that shows symptoms of known viruses.
- Comprehensive reports should be made available to track action and identify problems.

Lastly, the best defense against spreading viruses comes from network users themselves. Make sure that all users are aware of problems that can be caused by a successful attack. Those attacks can harm them in degrees that can range from inconvenience to lost wages. Users should be told to be very careful when opening email that comes from unknown or unexpected sources. Attachments should not be opened unless the user is confident of the source. They should also be told that software and data files brought from

outside the company should not be loaded on their workstations. Files may be infected or they may interfere with the ability of anti-virus software to do its job.

7.9. ATTACK RECOVERY

In the unlikely event that the dealership does suffer from an attack, the most important predictor of its ability to recover from that attack is the degree to which it prepared for that attack. The first step is to identify information that is pertinent to the operation of the dealership. That information should be copied (backed up) nightly. It is not necessary to backup all software as long as master copies are available if needed, but any configuration files or settings should be backed up when ever they change. Any data generated by dealership personnel MUST be backed up without question. This would include email folders and documents created on clients. Larger dealerships should consider storing that data on a central server. This will simplify the backup process and eliminate the need to have multiple users backing up their own data. It is always a smart idea to keep several generations of backup in case a file is lost or damaged and it is not noticed for several days.

Attack Recovery could be a full time job. Once a dealership decides to take on the responsibility of identifying and attacking this problem, it will most likely be the only activity that they could do. The Internet is constantly changing and there are new attacks and vulnerabilities that are being discovered daily. The best way to handle attacks is to partner with a company that has the resources available to handle it on an enterprise level.

7.10. RECOMMENDED POLICIES

Dealerships should establish a security policy and strictly enforce it. Users should be made aware of this policy upon initial access to dealership systems and be reminded on a periodic basis. Many companies use automatic pop-ups during login screens to remind employees of the corporate concern for security, and the ramifications of not following policy. Reference NADA Policy.

Table 7.1. Security Recommendations

Element	Description
Firewall/Packet Filters	MUST be used. Firewall and packet filtering capabilities within a router are sufficient
Personal Firewall Software	MUST be used on any machine that is mobile. Should be used on every PC in the dealership. Keep in mind the administrative costs
DMZ	Recommended for any network device or service that needs to be accessed from the public Internet2
Proxy Servers	Recommended for controlling outbound Internet access and URL filtering
Virtual Private Network (VPN)	Not required at this time but may be required by some OEMs in the future for secure two-way communication. Recommended for wireless LAN segments to protect data from unauthorized eavesdropping.
Intrusion Detection Software (IDS)	Recommended on a network level, but still requires a large amount of administration. From a PC perspective, it is better to implement IPS

Element	Description
Intrusion Prevention Software (IPS)	Recommend on a network level
Anti-Virus Software	MUST be used and updated regularly. Software should be used on all firewalls, servers, and clients to help prevent damage to dealership data
Wireless LAN	Recommend WPA V2 in an Enterprise and home environment. NOTE ** This replaces WEP technology that is widely being deployed today**
Attack Recovery	All critical dealership data should be backed up regularly and faithfully. A third party vendor should be used for real time attack recovery and prevention

7.11. USEFUL WEBSITES

- www.sans.org
- www.secinf.net
- www.grc.com
- www.av.ibm.com
- www.sarc.com

Chapter 8. DEALER MANAGEMENT SYSTEMS

Table of Contents

8.1. OVERVIEW

There are several important aspects of a DMS. Understanding and managing these key aspects can help determine how effective the DMS will be in achieving business goals. Demanding flexibility and open standards from the DMS will allow interaction with the myriad of applications and features that are available from a variety of sources, as well as utilizing the network infrastructure to its potential. Maintaining executive control and ownership of infrastructure and information will facilitate the ability to integrate with OEMs and third party suppliers. Following these guidelines will help preserve the dealer's customer relationship, ease the transition to new systems and suppliers and bolster competitiveness and innovation in the DMS market space. Look closely at the existing DMS and plan carefully when upgrading systems or changing suppliers.

8.2. DEALERSHIP NETWORK INFRASTRUCTURE

One of the main premises of the Dealership Infrastructure Guidelines is that the dealer maintains control and ownership of their network infrastructure. The dealer should also remain the primary decision maker. All application requirements should be compliant with the Dealership Infrastructure Guidelines.

Most applications can be accessed from the single dealership network, whether the application is from an OEM, DMS Provider, or a third party supplier. Dealers who maintain control over their network infrastructure will have greater flexibility and freedom to enhance their business with applications from a variety of sources.

8.3. TYPES OF DMS SYSTEMS

The Client-Server based DMS solution is comprised of a server and client PCs which are connected to the dealership LAN. In this solution the client PC actually does some application processing offering en-

hanced functionality. The server and related equipment are most often located and controlled in the dealership. In certain configurations remote access to the DMS is achieved via a WAN or VPN. Bandwidth requirements for this solution are moderate to heavy.

The Hybrid DMS configuration lets both PCs and green screens access the DMS. As the legacy terminal equipment becomes less feasible and more functionality is needed, users will move from terminal based green screens to networked PCs.

The ASP model DMS has a centrally located server which is accessed via the Internet or VPN. The DMS server is physically located and controlled outside of the dealership at the provider's hosting facility. Servers and infrastructure may be shared by other customers so the vendor must have security to prevent other customers from accessing your data. Data access is controlled by the DMS provider and the internet access providers. Any of them could impact access to dealership data if there are billing disputes or equipment failure. Bandwidth requirements are moderate to high as streaming video and picture content increase in applications.

8.4. ASSESSING THE EXISTING DMS

While preparing to work with DMS providers, the Needs Assessment in Appendix can be invaluable. Dealerships should use this worksheet to gather information about their existing infrastructure and their current and future computing needs. Whether a dealership chooses to work with a third party network service supplier or their DMS provider, the answers to these questions will provide the supplier with pertinent information. Using the assessment may just save the dealership a considerable amount of time and money when comparing supplier offerings. Examples of issues that need to be worked out between the dealership and the DMS Provider include:

- Does the DMS require a Domain Name Server?
- Is the dealership going to offer services outside the dealership?

For more information review the checklist in the appendix. Additions, modifications or updates to the DMS may be needed in order for it to be placed on the dealership's Internet enabled infrastructure. Through proper planning and coordination, the DMS can seamlessly migrate to the dealership Internet infrastructure.

8.5. CHANGING DMS PROVIDERS

Switching to a new DMS provider can be a daunting task. Having an effective plan in place when migrating to a new system can ease the burden but dealers should expect at least 6 months of transition time to learn a new system. Prior to making a change, dealers should determine if a new system will require major changes to their LAN, fit the workflow process of all departments in their store and if all of their customer information can be converted over to a new system.

Once a dealer has committed to changing systems, it is important to have the proper training to learn a new system. Dealers should consult with their new DMS providers to ensure that adequate training is provided to help ease the transition period.

If a dealer is considering a change to a new DMS provider, it is important that they do as much research as possible before making a final decision.

8.6. WHAT DMS PROVIDERS CAN DO

DMS providers have been installing and supporting dealership applications for years. Some DMS providers offer a range of services from software only to complete LAN solutions including design and installation. Those DMS providers are also extending their product and service lines to include Internet based solutions. The DMS provider can be a valuable resource when the dealer is considering a change to their network infrastructure.

8.6.1. Assessing DMS and Third Party Provider Offerings

The dealership has a large number of choices when deciding which network supplier to use when implementing the dealership infrastructure. Along with the countless network suppliers, many of the DMS providers offer product lines or packages that allow the dealership to connect to the Internet. Review all offerings carefully to ensure adherence to the DIG and its open standards.

When considering Internet enabled infrastructures, make sure the network supplier's offering will support the dealership requirements. The following are points that should be addressed when reviewing a network supplier's offer.

While some decisions related to the network infrastructure may be necessary to meet security requirements, be sure to understand how each decision relates to the dealership’s overall system.

- Does the provider prevent the dealership from using its infrastructure for its own purposes? Some examples of these would be any provider who:
  - Requires a dedicated Internet connection for their ASP traffic only thus precluding any other dealership Internet traffic.
  - Requires a specific ISP be used in lieu of existing connections which may meet technical specifications.
  - Disallows third-party equipment to reside on the dealership LAN.
  - Uses support disclaimers as well as cost prohibition to enforce these restrictive scenarios.
- What are the general terms and conditions of the contract?
- Do the offerings require a long-term contract?
- Will installed wiring remain intact and be usable at the end of a contract term?
- Will the dealership have the option to own the equipment at the end of a contract term?
- Does the offering support the latest, most cost efficient technologies such as DSL, Cable, Wireless, etc?
- Does the supplier provide voice and data integration services? If so, to what extent?
- Can modifications be made to accommodate dealership specific requirements such as port assignments and services on routers and firewalls?

- What are the charges for modifications or additions?
- Does the dealership require a web server, mail server, DMZ, etc.?
- Are proxy services available?
- Can the dealer control decisions regarding access authentication and authorization?
- Is the DMS onsite or hosted externally (ASP)?
- Is the DMS compliant with all legal statutes related to safeguarding customer privacy? See Chapter 15, *SAFEGUARDING CUSTOMER INFORMATION* Chapter for more information on this topic.

Technologies are changing at a rapid pace and dealers should keep contracts short term such as ISP offerings which should be limited to one year. Infrastructure equipment and wiring offerings should be limited to three-year contracts.

When shopping for an Internet enabled infrastructure keep the DIG in mind. Ask the supplier if their infrastructure adheres to the guidelines. What open standards are followed by the offering? Beware of phrases in any offering such as "unique dealership" or "specialized" that might point to a proprietary solution. Be wary of bundled solutions that have no separate network costs. These solutions might seem attractive, however if the dealership decides to change Internet carriers, or network companies, the whole LAN might have to be removed and reinstalled.

With ASP model DMS systems, particular attention must be paid to the method of Internet connection that is required for this system. Some vendors may use an existing Internet connection. Others will want to use their proprietary connection methods (Frame-relay, etc.). These proprietary connections (although not recommended) may be necessary for the DMS provider to meet SLA agreements with the dealership.

Proprietary offerings or solutions where the dealership does not control decisions about the infrastructure equipment can lock a dealership into an infrastructure that is neither flexible nor scalable. For instance, security is a critical component of an Internet enabled infrastructure. If a dealership does not maintain control of its security policy, the dealership can be at risk, unable to communicate with suppliers, or find some applications unusable. It is important to have the authority to easily and affordably make policy changes to the network firewall, content and spam filters.

Most importantly, dealerships must compare offerings so they receive competent, compliant and competitive proposals. Many companies and some OEM's may be offering certified solutions for Internet enabled infrastructures. While it may seem challenging to prepare for and find the right provider, the dealership will be rewarded with crucial flexibility and scalability by owning and controlling its own infrastructure.

If the dealership personnel are still uncomfortable with the offerings, check with an independent consultant or specialist. Independent consultants that are not associated with a particular supplier should be able to recommend various options and packages that meet all of a dealership's networking needs without bias toward any supplier.

8.7. DATA ACCESS

Knowing who is accessing DMS data and customer information and having a solid backup plan in place is critical for dealers to protect their customer information. With recently introduced rules and regulations regarding safeguarding customer data and privacy this is a matter that should be taken very seriously.

It is important for a dealer to know everyone who is accessing their DMS system for customer data. This includes OEM's as well as any third parties acquiring information to help the dealer with customer service, follow-up, etc. A dealer should also be aware of what information about their customers is being accessed, how it is being accessed and transmitted and what the other party is doing with the data once they receive it.

8.8. BACKUP

Another area of great importance is the backup of system data. For dealer's that have an onsite DMS server this should require a strict policy. Backups should be done on a frequent basis (daily is recommended). The transportation and location of the backup is also important. It is recommended that backup media be stored at a secure offsite location is case of acts of nature such as flooding, hurricanes, etc. A dealer should know which personnel are responsible for handling these steps in the event of an emergency.

For dealer's that utilize an offsite server or ASP solution with their DMS provider these backups are handled by the DMS provider in a secure manner.

Chapter 9. CLIENT HARDWARE REQUIREMENTS

Table of Contents

9.1. OVERVIEW

Client hardware in the dealership is the responsibility of each individual dealer. Each OEM establishes the minimum specifications necessary to run their corporate applications. While a dealer is free to choose any hardware, using client hardware that meets or exceeds these specifications will ensure that all OEM applications will run as expected. Procedures are in place for the dealers to order standard configurations from OEM's, PC vendors and value added resellers (VAR's). Details on the configurations and the ordering process are found in the addendum provided by each OEM.

9.1.1. Workstation set-up considerations

When considering client hardware purchases, clients should take into account other items outside of the computer itself. Standard workstation set-ups should include electrical Surge Protectors and Ethernet jacks for connection to the local network. These measures protect hardware investment and, taken in total with the hardware, they provide a reliable working environment. When modem or Ethernet ports on the PC are connected, they too should have surge protection as well. Many power surge protectors will also have jacks for the telephone and network lines. To meet or exceed power industry standards, protectors will be Underwriters Lab (UL) 1449 Listed and/or CSA Certified

Damage from power spikes is the number one cause of component failure in PC's. Even small surges can cause damage over time and lessen the life span of the equipment. Surge protectors can safeguard equipment against lightning and surge damage while reducing EMI/RFI line noise that can cause computer lockups and data errors. While an uninterruptible power supply (UPS) is generally not required for a client workstation, using a good surge protector is a necessity.

In locations where problem with frequent power outages, dealerships may want to consider taking extra steps to protect their equipment. UPS, line conditioners, and/or isolated electrical circuits can all be appropriate choices for given situations. A brownout condition can damage sensitive electronic devices due to reduced and fluctuating voltage levels. This situation will cause electronic components to operate outside the range they were designed to work in. A UPS has the ability to keep line voltage constant in low

power brownout conditions, while surge protectors are not designed to keep voltage constant in low power situations which are why they are less expensive than a UPS.

9.1.2. Selecting Client Hardware

Technological advancements in PC's include the Universal Serial Bus specification 2.0 (USB 2.0) which incorporates plug and play technology that can make connecting multiple external devices much easier, for example printers or keyboards. Additionally, multi-function drives have emerged that combine compact disk (CD) and digital versatile disk (DVD) drives into one drive. Multi-function drives can vary in their ability to read and or write CDs and DVDs. Check with your OEM to determine if you may receive software or data in a DVD format which requires a DVD or multi-function drive. The popularity of flat panel display is increasing because they require less space than traditional cathode ray tubes (CRTs) of the same screen size. When using flat panels that may require a DVI (Digital Video Interface) interface, check the video connector options on the PC for compatibility.

9.2. PC CLIENT USES

Several factors should be taken into account when deciding when and where to add Personal Computers (PCs) or to replace green-screen terminals. If a user only uses green screens, and the application will not be changing, there appears to be no need to place a PC at that location. On the other hand, if the applications they use will be browser based, then this green screen should be considered for replacement with a PC.

Another situation where replacement might make sense would include the substitution of one PC in place of multiple green screens. People who need to run browser-based applications, or users that require multiple applications from possibly dissimilar networks, are candidates for PCs.

The schedule for the business system providers to convert to browser-based applications is also an important consideration. Given the current rate of change in the PC industry, a PC's useful lifespan is approximately three years. After this time, consider refreshing and or replacing PCs.

9.2.1. Service Contract Considerations

While every new PC comes with a warranty, the duration and terms can vary greatly. Vendors can provide carry-in, mail-in, and/or on site repair service. In business situations the downtime and the extra expense of hauling or shipping the computer off for service is unacceptable. On-site repair plans with reasonable response times are usually preferred. Providers and service plans targeted at home users will usually not provide an acceptable level of service for more demanding business users.

9.2.2. Browser Software

Software used to view web pages will be the core software element of each client. A browser loads and displays pages and provides basic web-navigation tools. The dominant browser packages are Microsoft Internet Explorer and Mozilla Firefox. Browser software is generally available without cost and updates to supported versions will be available for download using the web. Each OEM will provide details on supported versions in their addendum.

9.2.3. Anti-Virus Software

An unintended result of using the Internet is the possibility of infecting workstations with malicious computer programs. These programs are often referred to as viruses. A detailed plan to provide anti-virus protection across the entire local area network is contained in the Dealership Security chapter.

One piece of that plan involves the use of anti-virus software on the individual client. This software should scan incoming files in order to prevent new viruses from reaching the client. It should also search the hard drives and memory for viruses that may already be hidden there. Aggressive use of anti-virus software will reduce the chances of harming an individual workstation and it can help eliminate problems before they infect multiple workstations.

Scans for viruses should be run whenever workstations with extremely important data are started or rebooted. This can help avoid a new virus activating and destroying any data. Keeping anti-virus software up to date in order to detect new viruses is essential. This requires applying each update as the software maker releases them. The discovery of a new virus by the software maker will prompt a new update release. See the Dealership Security chapter for more details on possible solutions.

Chapter 10. HARDWARE PERIPHERALS

Table of Contents

10.1. OVERVIEW

Choosing products to work with business networks can be a daunting task and most small to medium size businesses do not have IT departments to make these complicated decisions. There are many factors that companies should look for when choosing items such as printers, faxes, uninterruptible power supplies and; back-up and recovery systems. This chapter is a compilation of checklists, considerations, and best practices regarding the implementation of network devices and computer peripherals in the office environment. (Dell)

There six are basic considerations for selecting any add-on to a computer network. They are:

1. **Ease of Use:** Is the device easy to install and run with little vendor support, or does it require a lot of training and experience or customer support?

2. **Reliability:** Does the product have a history of problems? What warranties and service contracts are available and what is the extent of the coverage and the contract duration?

3. **Performance and Speed:** How does a particular product perform in comparison to other similar products? How will it affect the speed and performance of the network?

4. **Cost of Ownership:** What is the initial cost and what is the cost over the lifetime of the product. Some products that are the least expensive in the beginning can be come very costly when consumables and service issues are factored into the equation.

5. **Depth of Feature Set:** What features are necessary and what features are available?

6. **Implementation Issues:** What operating systems is the item compatible with? What other equipment does the device affect? Are there any upgrade limitations for the equipment or any software programs installed on the equipment?

10.2. PREVENTING LOSS OF DATA

The two most common and critical server peripherals are usually a device to back up the files on your server and an uninterruptible power supply (UPS). The UPS will help to prevent both hardware and software damage which can result from fluctuating power levels and will allow any equipment plugged into it to run on its battery for a short period of time in the event of a power outage and allow the equipment to shut down. The backup device will allow you to make copies of important files like customer contact data as well as sales and service activity, separate from the server or other computers, to safeguard your company against loss of data which could result from computer failures. The UPS should be checked periodically.

10.2.1. Back-up and Recovery System

Look for the following in a back-up and recovery system:

- A product that can allow critical dealership information to be backed up and does not omit certain file types and equipment configurations.
- A product that has reliable schedules.
- A product that has reporting and comprehensive logging capabilities to record and send alerts to an administrator when something goes wrong.
- A software product that encrypts the backup archive with a minimum of 256 bit encryption.
- A software product that has bit-level validation.
- A software product that is easy to use and allows for easy data back-up and selective restore of the desired dealership business information and IT applications.

10.2.2. Uninterruptible Power Supply(UPS)

A UPS traditionally can perform the following functions to protect dealership computer, phone and security equipment:

- Absorb small power surges.
- Filter or block out electrical "noise" from power companies.
- Continue to provide power to equipment during power "brown outs".
- Provide power for some time after a power "blackout" has occurred.

UPS/software combinations can provide the following functions:

- Automatically shutdown equipment during long power outages.
- Monitor and log the status of the power supply.

- Display the voltage/current "drawn " by the equipment connected to it.
- Enable the equipment to be restarted after a long power outage.
- Display the voltage currently available.
- Provide audio alarms and send electronic messages to IT administrators when certain error conditions occur on the UPS.
- Provide protection against short circuits that could permanently damage computer equipment connected to the UPS.

Look for the following characteristics in a UPS when selecting replacement units:

- Sinusoidal power output. In general, the closer the AC output of the UPS is to a sine wave (not square wave patterns), the better the equipment.
- A manual bypass switch that allow you to pass power through the device if it is broken or being serviced. This would be for emergency situations since the critical UPS safety features would no longer be functioning.
- The ability to monitor how much power (or percentage load) the equipment is drawing, how much battery life is left and indications of the input power quality. Expectations for the power battery pack can range from 15 minutes to several hours. If more back-up time is needed, then solutions that include a diesel generator should be considered.
- The ability to communicate with the UPS monitoring software via a network connection and also SNMP.
- Make sure the wattage of the device and the power source circuit breaker are compatible. Look for the UPS volt-ampere rating.
- A good support/maintenance contract that includes a 4-hour on site response time and/or overnight shipment of a replacement UPS unit.

The following are recommendations for maintaining a UPS:

- Perform regular maintenance on the UPS and change the batteries periodically as recommended by the UPS manufacturer. Do not "deep cycle" the batteries any more than is necessary.
- Make sure the UPS keeps in contact with its electrical ground at all times.
- Do not subject the UPS to temperature or humidity extremes, water, excessive dust, or excessive static electricity. Keep the area around the UPS clean and dry.
- Do not overload the UPS. Ensure the maximum power rating for all equipment connected to the UPS unit is well below the UPS unit's maximum power output.
- Test the system regularly by simulating an outage. If the UPS shows signs of misbehavior or malfunction, remove it from service at the earliest possible opportunity. Don't put it back into service until it has been examined and recertified by qualified UPS service personnel.

10.3. PRINTERS

Selecting a printer includes more than consideration for the cost and functionality. Data privacy and security issues also need to be addressed. This section will deal with how to select a printer for the dealership’s needs and the best practices for implementing both the functional and security needs of the dealership.

Printer selection criteria:

- Technology is the first factor to consider when purchasing a printer. There are two types:
  - Inkjet printers are affordable and effective for home and the dealership.
  - Laser printers are recommended for dealerships that require speed, efficiency, and high quality color or black and white printed resolution.
- Printer resolution is measured by the number of dots per inch (DPI) a printer is capable of printing. It is important to compare the DPI of the printers being evaluated.
- The speed of a printer is rated in pages per minute (PPM) and range from 4 and 10+ PPM. Speed depends on several factors including if it is black and white or color, text only or full page graphics. Expect a faster PPM from a laser printer printing text rather than graphics. A laser is always faster and has lower maintenance than an inkjet printer.
- Ink or toner is a key factor in determining total cost over the lifetime and level of satisfaction regarding printers. Three factors should be considered:
  - Price – in general the price of the ink can far surpass the price of the printer. Consider how much the ink will cost, the number of pages it should yield, and the estimated cost per page. The manufacturer/distributor should include this in the general product information.
  - Availability - some printer manufacturers may require that you purchase their brand of ink A substitute ink purchased from a third-party may cause your printer warranty to be voided. Verify what brands of ink can be used and also can be purchased from a third-party.
  - Type - consider what type of ink or toner is used with your printer. Users considering an ink jet printer should check if the printer model requires separate color cartridges. Some products may include multiple colors in a single print cartridge. If so when only one color runs out the entire cartridge must be replaced. Also, check if the cartridges are just ink or a combination of ink and separate nozzles. Cartridges with ink and nozzles will cost more than those that have just ink..
- Cost Per Page is the estimated ongoing cost of the printer after its initial purchase. It is important to look at the cost per page and see how much you may be paying for the anticipated print volume. Generally laser printers' per page cost is less than that of ink jet printers..
- Paper handling - the method of how the printer handles and distributes the paper can be an important consideration when looking at printers. Many Ink Jet printers will feed paper through a slot on the top of the printer while laser printers will use a tray method of feeding the paper to the printer. Depending upon the amount of printing you expect to have and the type of paper you plan on using, such as a paper envelope will help make your decision when purchasing a printer.

- Options - Check to see if the printer requires add-ons that would increase the overall cost of the printer. All-In-One devices are becoming more popular for small businesses. These printers have the ability to make copies, scan documents and in some cases act as a fax machine. Questions to ask to determine the need for any options include:
  - Will those using the printer print a lot of reports?
  - Will they be single copies or multiple sets of printed copies?
  - What is the estimated average quantity of each?
  - What is the estimated total printing workload per week and per month?
  - Are there any critical peak periods of printing, both attended and unattended? If so what is the required printer production (printed page count)?
  - What are the range of size requirements and will the printers support those requirements?
  - Will the printer be able to handle special forms containing adhesives such as labels or other composition that could destroy the printer?
  - Will the printer output be “read” by dealership staff, customers, or special scanners?
  - How attractive do the labels, reports, and dealership letterhead need to look?
  - How durable should the labels and printed display notices be?
  - Who will see/scan these printed documents? Customers or are they only used internally?
  - What are print quality requirements for all of the printing jobs?
  - What “hold print” security features are needed to protect confidential report content?
- Price Range - the price range can vary depending upon the quality of the printer, the type of printer, the print speed, and whether it only prints black and white or also color. A general price range follows:
  - Ink Jet Printer $100.00 - $400.00
  - Laser Printer $300.00 - $2,000.00+
- Printer Traffic - who will use the printer? Network printers are the best option when several people have light-to-medium printing needs. However if individual employees will be printing a substantial amount it may be wise to put a dedicated non-network printer at near their workarea.

10.4. PHYSICAL SECURITY FOR PRINTERS

A printer located in a public place opens the risk of giving unauthorized people access to confidential information when documents are left on or near the printer. Also, intruders may be able to access documents by hacking into the printer's spooling device or by utilizing a reprint feature on the printer.

Recommendations

The following recommendations can reduce security risks associated with printers and their printed documents:

- Avoid locating printers in public places.
- Emphasize to dealership staff the importance of always protecting confidential printed documents.
- Include all printers when developing and periodically reviewing the dealership's physical security procedures.
- Schedule the printing of highly confidential documents to ensure the designated printer is available. If the printer does not have a confidential print queue to "hold" the documents until released, then have an authorized person stay at the printer while it prints.
- In some cases, employees that need to print a substantial amount of confidential and/or sensitive data should have their own non-network printer in a secure location very near their workarea.

Basic Printer Etiquette

Anytime multiple people are using a central device there is potential for conflict and frustration. Basic printer etiquette is not just about good manners; it helps ensure a business functions smoothly. Because of this many business apply printer etiquette policies to avoid conflict. Common requirements are:

- If you print job uses all the paper fill it up.
- If the printer runs out of ink, refill it.
- If there's a paper jam, follow the directions and try to clear it out or get assistance.
- Print large file at off peak time or use a low traffic printer. Some printers will allow you to schedule print jobs at specific times so it is possible to print after business hours.
- Avoid picking up other peoples print jobs and leave the pages in order.

Fax Machine Considerations

There are several fax options:

- The traditional fax machine hooked up to a dedicated phone line that requires paper and toner dedicated to that machine
- A fax as part of an All-In-One device where the printer and the fax are the same input and output device
- An online fax service that gives you a virtual fax number and all outgoing faxes are sent from a PC and incoming faxes are received by email
- The fax modem which allows documents to be scanned and directly faxed from a PC
- A fax server that works over the network

Traditional Fax machines carry similar risk to privacy and confidentiality when used in community setting. As with a printer, users who utilize a heavy load of sensitive faxed data should have their own dedicated fax machine in a secure location.

Modern fax modems that are in most late model PCs have the ability to send a fax to either a fax machine or an email address. For some sensitive data the later may be the better choice.

10.5. TABLET PCs

Tablet PCs are fully-functional laptop computers. They may include touch-sensitive screens designed to interact with a digital pen or a person's fingers. The pen or finger replaces the mouse and/or keyboard and can do things like select, drag, open files, allow for handwritten notes and communication.

Tablet PCs have advantages and disadvantages compared to laptops and desktop units.

Advantages:

- They do not interrupt line of sight since they lie flat on the table.
- They can be held in one arm while standing and giving a presentation.
- They can be used like a book or notepad.
- Some users aren't comfortable with keyboards, and like the ease of entering text through handwriting.

Disadvantages:

- They may cost more than their non-tablet counterparts.
- Tablet PCs may be less powerful than traditional laptops.
- The size of Tablet PC screens may be smaller.
- There is more strain on the hinge in convertible Tablet PCs, than on traditional laptops.

Things to look for and features to compare when considering a Tablet PC are:

- Portability
- Wireless Capability
- Handwriting and Speech Recognition Capability.
- Battery Life
- Security options

10.6. Payment Gateways and Credit Card Processing Device

Credit Card Processing enables businesses to expand payment options and therefore may increase revenue. Below are features that should be evaulated when choosing Payment Gateways and credit card processing devices and service providers:

- SSL Security - socket Level Security with a high level of encryption
- Fast processing speed - authorization responses should be 10 seconds or less
- Multi-currency support: - offers the ability to accept payments from other countries.
- Application transparency - keeps the domain name (URL) pointed to your site to avoid customer concerns over security.
- Full, partial and blind credits - allows you to issue refunds for the full amount, part of the original amount and in the absence of an original transaction through a secure web interface.
- Email notification options - enables customers and/or merchants to receive an email once a payment has been made.
- Customizable email - allows merchants to create the content of the emails that will be sent to customers for successful or denied transactions.
- AVS Support - configurable settings that let merchants define the degree to which billing address info needs to match that on file with the cardholder's bank prior to approving the transaction.
- CVV2/CVC2 Support - reduces the risk of fraud by requiring that the codes on the back of VISA and MasterCard credit cards be entered into the payment form for verification. Web-based Reporting Access to standard and customized reports via a standard web browser.
- Transaction Management - provides a browser-accessible method of voiding, crediting, reauthorizing and setting transactions, as well as viewing transaction level detail.
- Multiple settlement options - enables scheduled automatic transactions settlement on a manual basis.
- Support availability - technical resources readily available to answer your questions with respect to transaction processing.
- Data redundancy - robust technical infrastructure, including redundant servers, connectivity and redundant data center. Eliminates risk of data loss.
- All stored or saved account numbers must be encrypted when stored and masked when displayed.
- All paper-based CC transactions such as mail back forms or faxes must be secured in a locking cabinet or other secure method and then properly destroyed once processing is complete.

10.7. SOLID STATE DRIVES

A solid-state disk/drive (SSD) is a data storage device that uses solid-state memory to store data. Unlike hard disk drives, which have spinning platters and drive heads, solid state drives should contain no moving parts. For dealerships, this may be an area for consideration for systems that require instant ‘on’ capability, or for portable systems in an abusive environment

SSDs may be preferred over traditional disk drives for a number of reasons. One advantage is in the speed of booting-up; hard disk drives need to be spinning and therefore have a "spin up" time which solid state drives do not. In addition, information on solid state drives can be accessed immediately so there is no de-

lay experienced when data is transferred. The data captured in SSDs is stored in memory and can be accessible almost instantaneously. The storage on SSDs is handled by flash memory chips, which provides three strong advantages: less power usage, faster data access and higher reliability.

Advantages:

- Faster start-up because no spin-up is required.
- Fast random access because there is no read/write head.
- Silent operation due to the lack of moving parts.
- Low power consumption and generate little heat when in use.
- Greater mechanical reliability due to lack of moving parts.
- Ability to endure extreme shock, high altitude, vibration and extremes of temperature. This makes SSDs useful for laptops, mobile computers, and devices that operate in extreme conditions.
- Failures occur less frequently while writing/erasing data, which means there is a lower chance of irrecoverable data damage.

Disadvantages:

- The capacity of SSDs is currently lower than that of hard drives. However, flash SSD capacity is predicted to increase rapidly.
- Asymmetric read vs. write performance can cause problems with certain functions where the read and write operations are expected to be completed in a similar timeframe. SSDs currently have a much slower write performance compared to their read performance.
- Due to the low storage density of SSDs, hard disks can store more data per unit volume than DRAM or flash SSDs, except for very low capacity/small devices.
- Flash-memory cells have limited lifetimes and will often wear out after 1,000 to 10,000 write cycles for MLC, and up to 100,000 write cycles for SLC. Special file systems or firmware designs can mitigate this problem by spreading writes over the entire device, called wear leveling.
- As a result of wear leveling and write combining, the performance of SSDs degrades with use.
- DRAM-based SSDs (but not flash-based SSDs) require more power than hard disks, when operating; they still use power when the computer is turned off, while hard disks do not.

SSDs are greater in cost when compared to hard disks. SSDs are a higher cost per megabyte of storage and are more expensive per gigabyte compared to hard drives. A normal flash drive may cost US $1.50-3.45 per gigabyte, hard drives are around US$0.38 per gigabyte. But in some applications the overall cost turns out to be less costly when comparing the higher reliability and no spinning parts of SSDs to the cost of possibly having to replace multiple hard disks.

SSDs are a rapidly developing technology that may be significant to how a dealerships data infrastructure is developed and managed. Understanding the full range of uses, advantages, disadvantages and costs of

SSDs should be considered when evaluating the different types of data storage within dealerships. Some applications within the dealers infrastructure may benefit from SSD like active directory servers or other applications where immediate booting-up would be required. SSD will however not replace data storage where a great deal of data writes are required like database servers or email systems.

10.8. SMART PHONES

A smartphone is a mobile [http://en.wikipedia.org/wiki/Mobile_phone] phone that offers more advanced computing ability and connectivity than a basic 'feature phone' [http://en.wikipedia.org/wiki/Feature_phone]. Smartphones and feature phones may be thought of as handheld computers integrated within a mobile telephone, but feature phones run applications on platforms developed to support phones. Smartphones on the other hand run on a complete operating system [http://en.wikipedia.org/wiki/Operating_system] software providing a robust platform for application developers.

Demand continues for smartphones that are more powerful than the previous versions and are equipped with faster processors [http://en.wikipedia.org/wiki/Microprocessor], more memory [http://en.wikipedia.org/wiki/Non-volatile_memory], larger color screens and open operating systems. Their rate of adoption has far outpaced the rest of the mobile phone market for several years. A recent study determined that smartphones would outnumber regular phones by 2015. Most smartphones are equipped with one of the following operating systems: Android [http://en.wikipedia.org/wiki/Android_(operating_system)], BlackBerry OS [http://en.wikipedia.org/wiki/BlackBerry_OS], iOS [http://en.wikipedia.org/wiki/IOS_(Apple)], and Windows Mobile [http://en.wikipedia.org/wiki/Windows_Mobile].

The feature rich smartphones enable the consumer to always be connected to the internet for access to email, texting, social media sites, videos, as well as phone services. An increasing number of automotive vehicles include wireless or Bluetooth features to “link” the smartphone to the vehicle’s infotainment features.

Retailers and manufacturers will have additional opportunities to communicate with their customers relative to their transportation and vehicle servicing needs. The communications will be able to be tailored to each customer’s preferences. With customers accessing social media sites and location-based services in increasing numbers retailers and manufacturers have new “locations” and methods of providing targeted, time-sensitive marketing advertisements to customers.

Advantages:

- By freeing you from your desk, smartphones enable you to send and receive communications from customers, employees, and business partners wherever you are, resulting in better customer service and faster business results.
- Provides the ability to contact the customer “directly” utilizing their preferred method of contact.

Disadvantages:

- Smartphones share many of the same security risks of laptops and are easier to lose, putting corporate information at risk. Best practices around securing smartphones are still emerging, but they need to be managed the same as PCs, and should be included in any comprehensive plan for the maintenance and security of the dealership IT infrastructure.

10.9. VOIP PHONES

VoIP is technology that allows two-way voice communications over an IP data network such as the Internet, enterprise IP connections, WANs or LANs. Traditional phone equipment can be hooked up to specialized devices which connect to the Internet or dedicated IP network. Voice calls are converted into data packets and sent to a VoIP service provider who converts them back and routes the calls to the Public Switched Telephone Network (PSTN). VoIP service may allow businesses to reduce or augment traditional local and long-distance voice services. Intra-company voice calling can be setup in a similar fashion via an IP based WAN without the need for PSTN connections or VoIP service providers. VoIP has the potential to offer substantial discounts for voice services. (VoIPReview)

Advantages:

- Less Expensive Phone Service - there is significant savings over traditional services.
- Affordable Long Distance and International Calling - long distance is included in most plans and international calls are at a nominal rate.
- Free Calling Features - including voice mail, caller ID, call conferencing, call waiting and call forwarding. VoIP users can have their voice mail messages e-mailed to them for easy playback and referencing. Also, consumers can adopt virtual numbers so local numbers can be created from remote places
- Convenience - customers have the ability to track their call activity, manage voice mail, view billing information, and change account information online at their convenience, 24 hours a day, 7 days a week.
- Mobility - most VoIP providers allow users to take their VoIP service with them anywhere in the world. With a high-speed Internet connection and the VoIP phone adapter, callers can place and accept VoIP calls from any location at any time at no additional charge.

Disadvantages:

- Some VoIP services don't function during power outages without battery backup.
- Some VoIP subscribers must manually enter their current address to be identified by a 911 dispatcher.
- Poor broadband Internet connections can cause call quality problems.

Great care should be taken when choosing a VoIP provider. There are two key considerations that outweigh cost factors:

- Performance - VoIP services provided by cable and telephone companies run over proprietary networks and therefore have less data packet interference and may have fewer problems.
- Service - many of the very low cost providers only provide customer service by phone. It may be wise to pay a little more to have technical support that is available to come out and diagnose problems onsite.

Chapter 11. DEALER DESKTOP MANAGEMENT

Table of Contents

11.1. OVERVIEW

Having a functional, efficient computer and network systems has become vital to most dealerships Original Equipment Manufacturers (OEMs), and Retail Service Providers (RSPs). The use of computers and the Internet has simplified essential tasks such as data creation, storage, access and exchange. However, the added conveniences, particularly of the Internet, have brought additional threats to individual computers and businesses as a whole.

As computer technology has advanced it has become less likely that problems with a system originate with the flaws in the computer's hardware. The introduction of malicious software to systems from the Internet and internal sources has become one of the biggest threats to information security and computer productivity. Malicious software is defined as any software that attempts to subvert the confidentiality, integrity or availability of a system. Spyware, viruses, worms, logic bombs, trapdoors, and Trojans are all considered malicious software. These unwanted intruders cause a variety problems, from slowing computer-processing speeds, which can reduce productivity, to outright stealing of privileged information, which could lead to liability.

Because the industry has become dependent on computer technology to conduct business, protection must be a priority. Desktop Management is a combination of products and solutions (i.e. Virus software, Anti-Spyware, Patch Management) to help facilitate keeping the desktop running at peak efficiency. These products do many things including protecting your personal computer (PC) from viruses and other malicious software to detecting patch application and operating system vulnerabilities.

This section will discuss the different types of malicious software, what effect they have on the PC, and what can be done to help prevent them from infecting a system. There are many products that help to protect against malicious software. Unfortunately there is no one, PC or server based, product that does it all. In this chapter, the DIG is going to examine the different tools and procedures that can be followed to help avoid these problems.

11.2. STANDARDIZING

A tremendous amount of time and effort can be saved by standardizing the equipment and software that is utilized by the dealership. This means that the majority, if not all, PCs in the dealership should be built on the same hardware and software platforms. Adopting this practice will streamline deployment and simplify training and support for users and staff.

These are some benefits of having standardized systems:

- Simplified Support - support staff is afforded greater familiarity with the common equipment and configurations which allows them to spend less time troubleshooting and more time fixing. Solving issues for multiple users or systems with one solution is cost effective and serves users better.

- Ease of Deployment - minimize effort when systems are installed or upgraded. Advanced testing allows staff to predict the impact on users and avoid lengthy down time and prolonged installations.

- Facilitates use of techniques such as disk imaging and cloning to allow systems to be setup and restored quickly.

11.3. TYPES OF MALICIOUS SOFTWARE

Malicious software is any software that the user did not authorize to be loaded or software that collects data about a user without their permission. The following is a list of terminology commonly used to describe the various types of malicious software:

- Spyware- Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a Spybot or tracking software), Spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.

- Virus- a virus is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document. Viruses can be transmitted as attachments to an e-mail note or in a downloaded file, or be present on a diskette or CD

- Worm- a worm is a self-replicating virus that does not alter files but duplicates itself. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

- Logic bomb- a logic bomb is programming code, inserted surreptitiously or intentionally, that is designed to execute (or "explode") under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command. It is in effect a delayed-action computer virus or Trojan horse. A logic bomb, when "exploded," may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects.

- Trapdoor- is a method of gaining access to some part of a system other than by the normal procedure (e.g. gaining access without having to supply a password). Hackers who successfully penetrate a sys-

tem may insert trapdoors to allow them entry at a later date, even if the vulnerability that they originally exploited is closed. There have also been instances of system developers leaving debug trapdoors in software, which are then discovered and exploited by hackers.

- Trojan (Trojan Horse)- a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the certain area on your hard disk. A Trojan horse may be widely redistributed as part of a computer virus.

- RATs (Remote Admin Trojans) - are a special form of Trojan Horse that allows remote control over a machine. These programs are used to steal passwords and other sensitive information. Although they are "invisible", symptoms such as a slow moving system, CD ports opening and closing and unexplained restarting of your computer may manifest.

- Malware - Malware (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also Spyware, programming that gathers information about a computer user without permission.

- Mobile Malicious Code - web documents often have server-supplied code associated with them which executes inside the web browser. This active content allows information servers to customize the presentation of their information, but also provides a mechanism to attack systems running a client browser. Mobile malicious code may arrive at a site through active content such as JavaScript, Java Applets and ActiveX controls or through Plug-ins.

- Malicious Font - webpage text that exploits the default method used to de-compress Embedded Open Type Fonts in Windows based programs including Internet Explorer and Outlook. These malicious fonts are designed to trigger a buffer overflow which will disable the security on Windows-based PCs. This allows an intruder to take complete control of the affected computer and remotely execute destructive activities including installing unauthorized programs and manipulating data.

- Rootkits - Rootkits are a set of software tools used by an intruder to gain and maintain access to a computer system without the user's knowledge. These tools conceal covert running processes, files and system data making them difficult to detect. There are rootkits to penetrate a wide variety of operating systems including Linux, Solaris and versions of Microsoft Windows. A computer with rootkits on it is called a rooted computer.

  There are three types of rootkits. Below is a description of the characteristics of each:

  - Kernel Rootkits - hide a backdoor on a computer system by using modified code to add or replace a portion of the system's existing kernel code. Usually the new code is added to the kernel via a device driver or loadable module. Kernel rootkits can be especially dangerous because they can be difficult to detect without appropriate software.

  - Library Rootkits - hide information about the intruder by manipulating system calls with patches, hooks, or replacements.

  - Application Rootkits - replace or modify regular application binaries with camouflaged fakes, hooks, patches, or injected code.

11.4. MALICIOUS SOFTWARE COUNTER-MEASURES

Attacks using malicious software are growing in number and sophistication. Antivirus, Anti-Spyware and other protection products continue to play a game of catch-up. New, increasingly complex variations are continuously being introduced and can sometimes spread widely before protection software companies deliver the latest detection strings and solutions.

Dealerships need to develop a malicious software strategy that clearly outlines the objectives and procedures for malicious software control and recovery. Introducing security measures can involve some risk and these practices should be done under the advice of qualified dealer network management.

- Security Awareness- user awareness is one of the most powerful countermeasures in virus control. Data should only be accepted from trusted sources. Users should be warned not to open suspicious email or visit 'hostile' websites. Furthermore, users should not be free to introduce unchecked media on to systems.

- Patch Management- patch management is the process of updating your servers or PCs with the latest security patches and service packs. Writers of viruses, spyware and other malicious software exploit existing flaws in software loaded on a PC to spread and do damage. Software companies will issue patches to fix flaws once they have been discovered. Using automatic updates to detect available patches for security vulnerabilities is vital to maintaining proper system functioning. However, there are times when installing a patch or update may actually interfere with current processes. Therefore, avoid automatic installation options. Use the following process to manage automatic updates:

  - Detect - use automatic updates to scan your systems for missing security patches and trigger the patch management process.

  - Assess - determine the severity of the issue(s) addressed by the patch and any other factors that may influence your decision, balancing the severity of the issue and mitigating factors to determine if the vulnerabilities are a threat to your current environment.

  - Acquire - if the vulnerability is not addressed by the security measures already in place, download the patch for testing.

  - Test - install the patch on a test system to verify the ramifications of the update against your production configuration.

  - Deploy - deploy the patch to production computers. Make sure your applications are not affected. Employ your rollback or backup restore plan if needed.

  - Maintain - subscribe to notifications that alert you to vulnerabilities as they are reported.

- Anti-virus scanners - these products scan files and email and instant messaging programs for signature patterns that match known malicious software. Since new viruses are continually emerging, these products can only be effective if they are regularly updated with the latest virus signatures. See your product manual for instructions on how to activate this. Anti-virus scanners can be positioned on gateways to the network and/or on network hosts. Anti-virus scanners need to be frequently updated to be effec-

tive. Therefore, regularity and method of update are criteria that need to be considered when selecting anti-virus products.

- Audit information - audit logs, including firewall logs, may detect abnormal activity. Examples are Trojans attempting to send data from a site, or malicious programs attempting to write or read to unauthorized areas.
- System hardening - careful implementation of system access controls, and the policy of running applications with least privilege, can minimize the damage caused by malicious software. This needs to be coupled with tight configuration management procedures.
- Active Content Blocking - blocks unwanted internet traffic and protects the network from malicious content on websites and spam emails. It also helps ensure business resources are being used for business purposed. There are four things you should look for in an internet blocking or filtering system:
  - Automatic Updates
  - Centralized Administration
  - Category Based Products
  - Reporting Capabilities
- Firewalls - firewalls can restrict the ability of some remote control programs to execute if they rely on a port that is generally blocked. A firewall can be either PC or server based. Firewalls are most effective at the Internet's point of entry. However, not a large degree of reliance can be placed on firewalls for malicious software control unless a gateway incorporates an active content filter.

11.5. RECOVERY AND CONTAINMENT

A recovery and containment procedure should be developed as part of an organization's malicious software strategy. The recovery procedure should also outline the process for making users aware of their requirements to report and act in the event of a virus contamination.

The principle requirements of a recovery procedure are:

- The ability to isolate infected systems. Otimally, when a threat is detected specific user's application sessions will be shut down and the user or network manager will be notified that an infection has occurred.
- The ability to purge malicious software from a system. Protection software should be able to regularly identify and remove harmful software that has invaded the system.
- The ability to restore the integrity of a system after an attack has occurred. Original installation disks or back-up data should be retained so data can be reloaded if corruption occurs.
- The recovery procedure must be clearly documented and regularly tested. For more information on network maintenance and checklist refer to chapters 2 and 3 of this manual.
- Refer to Chapter 16, Disaster Recovery and Business Continuation, for more information on implementing backup and restore procedures.

11.6. SELECTING SECURITY PRODUCTS

There are a wide variety of security products that can be incorporated into your overall security plan. Below are some of the key requirements to look for in different types of protection.

Patch Management Software:

- Regular scans of your systems for missing security patches.
- Automated so that detection will trigger the patch management process.

Anti-virus, Anti-Spyware and other Protection Software:

- Regular updates of Virus or Spyware definitions.
- Prompt updates for any new and rapidly spreading Virus or Spyware.
- A quarantine location for malicious software.
- The ability scan compressed files or folders.
- Reliable and ongoing support for the product.

Active Content Filter:

- The ability to recognize the increasingly wide variety of active content.
- An audit log describing the active content found and the action taken.

Both PC and Server based security options are available. Generally server based security products, particularly for anti-virus and Spyware, are considered superior because they block threats before they reach the individual PC level. However, server based products have an increased degree of complexity and need to be administered by qualified network management.

With the increasing threats to you networks and individual PC's it is tempting to install as many security products as possible. In theory this sounds like a good idea, however, installing multiple competing products can lead to serious problems. When changing brands or vendors make sure previous versions are uninstalled.

In networks that use centralized administration all servers, services and computing resources including support staff are located in centralized data center. This data center may be onsite or in some cases such as large OEMs located remotely. Centralized administration offers the best control over change management, version control, security management and other service continuity management issues. However, reliable high bandwidth WAN links to all sites will be necessary to deploy this type of network management.

More information on these subjects can be found on the NADA website at the following link: Http://www.nada.org

11.6.1. Password Protection

Passwords protect your data by limiting access to a single user or group or users. To keep privileged company information secure it is recommended that employees apply the following rules when creating and maintaining their passwords:

Do:

- Use a password with mixed-case alphabetic characters, numbers, and symbols.
- Use a mnemonic device that is easy to remember but hard to decipher. An example is IL2ccSitW (I love to cross-country ski in the winter)
- Change passwords every 30 to 90 days.
- Use a password that is at least eight or more characters (never use less than six).

Do NOT:

- Write your password down.
- Reuse old passwords.
- Share passwords with anyone.
- Allow group accounts with a common password.
- Use any of the following as your password:
  - Your login name.
  - Your first, middle, last name or nickname.
  - The names of your family members.
  - License plate or driver's license numbers, phone numbers, social security numbers, makes of cars or street names.
  - A single number or letter in a series (111111, aaaaaa, etc.)
  - Consecutive numbers or letters (123456, abcdef, etc.)
  - "Keyboard progression" passwords (qwertyui, lkjhgfds, etc.)
  - Numbers at the beginning or end of passwords.
  - A word from any dictionary in any language.
  - Fictional characters (especially fantasy or sci-fi characters, i.e., Luke Skywalker)
  - Names of computers or computer systems.

- Any user name in any form, such as capitalized, doubled, reversed, etc.
- Slang words, obscenities, technical terms, jargon, university slogans (Go Longhorns, Giggem Aggies, etc.)
- Any common phrase (Thank goodness it's Friday, Go ahead make my day, etc.).
- Any object easily spotted from your workstation.
- Any information about you that is known or can be learned (favorites - color, sport, TV show, etc.)

11.6.2. Phishing

A phish is a disguised email sent with the intent of obtaining privileged information. Phishing is widely used for identity and data theft.

Below is a typical example of how phishing would work in a business setting:

A user within a dealership receives an email which appears to be sent from the internal human resources or info-tech department. The worker is asked to click on a link or go to a specific website to update his user name and password or risk suspension. If the hackers receive the information they have access to the secure network along with any sensitive data it might contain.

Below are some guidelines to protect you from responding to these e-mails and revealing sensitive or private information:

- Know what is an inappropriate request for information. Below are some items that should never be given out in response to an email:
  - Your social security number or tax identification number
  - Your bank account information, credit card number, PIN number, or credit card security code (including "updates" to any of the above)
  - Your mother's maiden name or other information to identify you (such as your birth city or your favorite pet's name)
  - Your password
- Be on the lookout for poor grammar or typographical errors. Many phishing e-mails are translated from other languages or are sent without being proof-read and can contain bad grammar or typographical errors.
- Check the return address to determine if the e-mail may be from a "phisher". Genuine e-mails come from trusted e-mail addresses. While phishers often send forged e-mail to make it look like it comes from your organization, you can frequently determine whether it's authentic by checking the return address. If the "from" line of the e-mail ends with any domain other than that of your organization or one of your business partners, it may be fraudulent e-mail. Most e-mail clients let you examine the source of the e-mail. Check the information to see that the "received from," "reply to," and "return path" for the e-mail comes from your organization's domain or that of a business partner. The method you use to check the header information varies depending upon the e-mail client you use.

- Check the Web site address. Some phishers set up spoofed web sites that contain the name of your organization somewhere in the URL. Know the proper form of your organization's URL and extensions.
- Check the source of the e-mail. Some phishing e-mails include a link that looks as though it will take you to your account, but it is really a shortened link to a completely different Web site. If you "mouse over" the link with your mouse when viewing the message in your e-mail client, you often can see the underlying false Web address, either as a pop-up or as information in the browser status bar at the bottom of your internet window.
- Go directly to your account to review or make any changes to the account. Only open links from trusted sources. Avoid clicking on links contained in emails sent from unknown or suspicious sources. When in doubt verify with the sender that request is valid.

11.6.3. Plug-Ins and Multimedia Products

Plug-ins and Multi-media products provide streaming video, audio animation, instant messages and other services that can be extremely beneficial to your organization. However these products also provide additional risk of exposure to malicious threats and an increased use of bandwidth. The decision to install these products should be made in conjunction with your organizations network management. For more information about these products consult the Multimedia Delivery Chapter of this manual.

11.7. SOFTWARE PIRACY

Software piracy is the unauthorized copying or distribution of copyrighted software. When you purchase software, you are actually purchasing a license to use it, not the actual software. The license is what tells you how many times you can install the software. If you make more copies of the software than the license permits, you are breaking the law. Whenever you are copying, downloading, sharing, selling, or installing multiple copies of software onto personal or work computers, you are committing software piracy.[Ref_Software_Piracy_Definition]

Types of Software Piracy include:

1. Softlifting: purchasing a single licensed copy of software and loading it onto several computers contrary to the license terms.
2. Uploading and downloading: making unauthorized copies of copyrighted software available to end users connected by modem to online service providers and/or the Internet.
3. Software counterfeiting: illegally duplicating and selling copyrighted software in a form designed to make it appear legitimate.
4. OEM unbundling: selling standalone software that was intended to be bundled with specific accompanying hardware.
5. Hard disk loading: installing unauthorized copies of software onto the hard disks of personal computers, often as an incentive for the end user to buy the hardware from that particular hardware dealer.
6. Renting: unauthorized selling of software for temporary use.

[Ref_Software_Piracy_Types]

Using unlicensed software in your dealerships poses a significant risk to your dealership(s) in terms of potential fines, audit and legal fees, additional software licenses and maintenance fees, business disruption, and reputational damage. The risk of being audited by a software vendor has risen greatly in recent years, and the consequences can be substantial.

For dealers the best way to avoid being fined for software piracy is to develop an internal software management plan. Though this can be complex, resource consuming, and frustrating, the software purchaser is responsible for complying with the software license agreement. Internal auditors can help reduce the risk of adverse software audits by ensuring that an asset-management process has been implemented and that the dealership is prepared for a possible audit. As part of the software asset-management plan, the organization should review all software license agreements, perform a self-audit, and correct identified licensing deficiencies.[Ref_Software_Piracy_Audit]

Chapter 12. MULTIMEDIA DELIVERY

Table of Contents

12.1. OVERVIEW

With a business climate notable for rapid change, dealer owner/operators contend with reduced cycle time and the need to continually adjust their operations to meet new product launches and emerging market conditions. Important training and marketing information can be effectively communicated using existing and new content delivery methods. Multimedia delivery is the distribution of rich multimedia content to users. Multimedia content is the presentation of integrated text, graphics, video, animation and sound.

OEMs and third parties deliver diverse types of multimedia content, through a variety of media. While CDs and DVDs remain popular, the internet also has become a primary means of distribution, via webinars, webcasts, chat sessions, blogs, and social media sites.

Inevitably the dealership will be presented with one or more types of multimedia content. Becoming familiar with different aspects of multimedia delivery and how it fits in the overall dealership infrastructure will help in preparing for the costs and logistics of implementation. Some Multimedia technologies can be bandwidth intensive making it difficult or impossible to function on low speed connections such as dial-up and may impact performance on shared connections.

12.2. MULTIMEDIA TECHNOLOGIES

Adobe Flash and Microsoft Silverlight are browser based animation technologies with optional audio and video. Bandwidth consumption ranges from low to high depending upon the amount of video and audio content used, and typically uses less bandwidth than traditional video files.

Streaming media technology delivers audio and video to the PC via the Internet. Streaming media is used for distance learning, corporate communications, and product training and marketing. Two common approaches to streaming media are “progressive download” and "true streaming". Streaming media files can be produced at different quality levels. The quality is in large part determined by the encoded bit rate. The higher the encoded bit rate the better the quality. Higher quality presentations will be larger in size causing a greater demand for bandwidth. . In some cases the user can select a presentation with lower bit rate which requires less bandwidth. However, this option will provide a lower quality presentation and may not be the best choice if attention to detail is needed.

Progressive download refers to online media that users can watch as the files are downloaded. Because progressive download material is placed on a standard HTTP or FTP server, it is easier to administer, and generally introduces fewer problems with firewalls. Progressive download is strictly an on-demand technology and does not work for live broadcasts. Progressive download delivery is well suited to short movies that you want to be viewed at high quality, such as movie trailers and product advertisements. Progressive download is not a good solution for long videos or material the user may want to randomly access, such as lectures, speeches or presentations. Progressive download caches the content so subsequent viewing will run locally, avoiding impact to the network and may allow media files to be saved for redistribution. Higher quality presentations will have longer download duration than those of lower quality. Higher quality presentations will have a greater delay allowing a portion of the content to cache before viewing begins. Progressive download may tie up a great deal of bandwidth during the download so it is suggested to this at times when computer activity among the users is lower. This option may be a good alternative for dealerships with lower bandwidth and when firewall constraints prevent streaming.

True streaming refers to technologies that deliver media in real-time. True streaming delivery is well suited to live events. It also supports random access of material, so the user can fast forward to other parts of the video. True streaming uses special network protocols, such as RTSP (Real-time Streaming Protocol), MMS (Microsoft Media Server) and RTMP (Real-Time Messaging Protocol). These protocols can sometimes have trouble with firewalls, so viewers may not be able to see true streaming material from certain locations. True streaming media requires special servers, these servers give you a greater level of control over media delivery but can be more complicated to set up and administer than a standard HTTP server. Higher quality presentations require proportionately more bandwidth because they stream in real time with a nominal amount of buffering. True streaming will use network resources each time they are viewed and typically cannot be saved and redistributed.

Popular types of streaming media are Real Systems Media, Windows Media, QuickTime and Flash Video.

Webinars (or eSeminars) and Webcasts are online tutorials and presentations which make use of one or more of the above technologies for delivering multimedia content. Browser plugins are usually required, and bandwidth and system memory usage will vary depending upon the technology, and the type and amount of content. Closing other applications while working with this content is usually good a precautionary step to avoid a system slowdown.

12.3. BROWSER PLUG-INS

12.3.1. Adding Plug-ins

As mentioned above, most online multimedia content types require brower plugins. Most web pages which require plugins for display and use of the content provide the user with a link or button to download the required plugins. Most plug-ins are free and, being relatively small programs, download quickly. Regardless of the browser you use, the procedure is basically the same. Multimedia content is delivered in various file types, each of which may require its own type of browser plug-in. If there is a specific technology that the dealership uses they may want to deploy the necessary plug-ins to all the machines at the same time rather than on an individual basis.

Downloading anything on the internet involves some risk. Only download from approved content vendors, or someone your trust. For security reasons you may want to obtain your plug-ins directly from the developer’s sites instead of clicking through on a website.

Plug-ins provide services that can be extremely beneficial to your organization. However these products also provide additional risk of exposure to malicious threats and an increased use of bandwidth. The decision to install these products should be made in conjunction with your organization's network management.

12.4. DELIVERY METHODS

Multimedia content can be delivered via the Internet, or by more traditional methods such as CDs and DVDs.

12.4.1. Traditional Delivery Methods

DVD video offers high quality full motion video in a standard format which can be viewed with a standard player and television. Multimedia CD/DVD can be played on most personal computers and may be used for video as well as any type of multimedia content which can be delivered online, These formats are portable for convenient viewing at different places at any time, but interactivity is limited. Delivery can take days or weeks via “snail mail” or shipping companies. Content distributed in this manner can become stale and updates may not be timely. This delivery method is more feasible at lower volumes.

12.4.2. Internet Multimedia

More and more frequently, multimedia content is being delivered via the internet in an ever-increasing list of ways, including public web sites, dealer portals, blogs, social media sites, and chat rooms. Online content can be accessed by a desktop PC for on demand viewing or downloaded locally for later viewing. Access is available anywhere at anytime subject to the constraints of the viewer’s Internet Service Provider (ISP) and/or Local Area Network (LAN) and the owner of the content. Control can be added to allow authorized users to access the appropriate content from a store location. A great deal of interactivity can be achieved with Internet technologies. Content can be fresh with timely updates but this method can be bandwidth intensive for the viewer’s local area network. Bandwidth consumption is relative to video quality and number of concurrent users on the same network. Open solution cache devices may help control overall bandwidth consumption by temporarily storing content locally.

12.5. RECOMMENDATIONS

No single recommendation can be made for Multimedia delivery. Decisions MUST be made on individual dealership needs as well as OEM and third parties offerings. Dealerships should consider the following criteria in determining if and how to make use of Multimedia content:

- Who will benefit from the content?
- Is access from outside the dealership required?
- Will multiple and/or simultaneous user access be required?
- What are the costs and requirements for the infrastructure needed to support the content?

Chapter 13. INTERNET ACCESS METHODS

Table of Contents

13.1. OVERVIEW

With the growth of the Internet, telephone companies and Internet Service Providers (ISP) have created numerous products offerings. The most promising offerings were evaluated to determine possible solutions for a dealership's Internet access needs. A summary of each these methods including their strengths is listed below.

Traditional network access has been offered in the form of dial-up, leased, satellite, or Integrated Services Digital Network (ISDN) products (ISDN has moved to more of a backup strategy, but is still a viable option) There is widespread availability of these methods.

Their capacities have range from low-speed 28.8Kbps dial-up (about 29,000 bits per second) to moderate speed 1.5Mbps leased lines (about 1.5 million bits a second).

Cost will vary depending on type and speed of access. Dial-up connections can use an existing telephone line with an inexpensive modem. ISDN and leased circuits require special connections and equipment and installation costs alone can approach $2,000. In addition monthly fees can be more than $1,000. Because these products have been available for some time, suppliers can easily match requirements to the various products. When searching for a product, make sure you check with different providers. These different providers can offer different pricing depending on the area and services available.

Emerging technologies can be found in newer products such as Digital Subscriber Line (DSL), aggregate dial-up, cable modems, wireless access, and enhanced satellite. These new products provide high capacity, ranging up to 10Mbps, at costs that rival older technologies. However, since development and deployment of these technologies is ongoing, availability is often poor and suppliers have difficulty matching products to needs. However as these products mature, those problems should be remedied. Also, when looking at these new solutions, verify that there is a Service Level Agreement (SLA) associated with the service.

At the end of this chapter, a recommendation is provided based on the overall strengths and weaknesses of each access method. It will help to decide which Internet connection method is right for the dealership. Individual decisions are guided by availability of service, capacity requirements, and cost for the dealership. Products with high ratios of bandwidth to costs, like DSL, are usually the most attractive but may not be available in some areas. Therefore, a more traditional service may have to be used. Because the market constantly offers new products, it would be wise to avoid any long-term commitments to connection services. Reviewing connection alternatives on a yearly basis will allow dealerships to take advantage of new products or downward shifts in current product pricing.

13.2. SERVICE LEVEL AGREEMENTS/QUALITY OF SERVICE

Businesses connecting their local networks to the Internet today are placing a great deal of attention on the Service Level Agreement (SLA) that they receive with their Internet connection. The SLA will detail the Quality of Service (QoS) that the provider offers with their service – in other words, their guarantee that the connection and the service will deliver as promised. In the past, suppliers have avoided making these kinds of guarantees. The large number of suppliers and a lack of coordination between them made it difficult to measure and track performance. As the Internet has matured, aggressive suppliers are concentrating more on customer service. Some Internet Service Providers (ISP's) now offer SLA's that differentiates them from competitors, and they can demand the same high-quality service from their suppliers. SLA's should cover such topics as connection availability, performance, and response time when outages or problems occur.

Connection availability is the amount of time that the connection is "up" and usable. Uptime figures usually exclude planned maintenance periods. Promised connection availability of 99.9% can be obtained. Standard SLA's usually offer something a few tenth of a percent less than that. SLA's designed for business users will have higher guarantees. Gray areas can exist when using separate Internet Service Providers and telephone carriers. An ISP may have a problem receiving traffic from the dealership. The dealer would consider the circuit unusable. The carrier may consider the line up if that the circuit is alive at both ends. Confusion over configuring and provisioning circuits is often blamed on the other supplier. It is best to combine elements of SLA’s so suppliers reselling services cannot hide behind another supplier’s lack of quality service.

Performance is measured both by the consistency of the connection and by the amount of data that can be sent using the connection (the bandwidth). Consistency guarantees are usually measured by the amount of latency on a connection. This is determined by sending traffic (called pinging) from one end of the network to the other. Performance SLA’s are restricted to the portion of the network that the carrier controls. Since the carrier is not providing a telephone or leased line directly from the dealership to the OEM’s data center, they must hand traffic off to other carriers. Once it has been handed off, the carrier will no longer guarantee its speed or even its safe arrival. Carrier SLA’s cover performance from the dealership router (the beginning of their network) to the point where they exchange traffic with other carriers (the end of their network). As a guideline, round-trip latency within the United States should be less than 85 milliseconds for wired connections. Watch the wording of performance SLA’s carefully. Find out how many exchange points traffic will have to go through. With the involvement of additional carriers and exchange points, the additional complexity can effect performance.

The bandwidth of the connection is measured by the amount of data that can be sent over the connection each second. SLA’s should clearly state the promised bandwidth. For connections that do not provide

consistent bandwidth, the guarantee should be based on minimum performance. If the connection does not provide equal bandwidth going to and from the dealership, both minimums should be listed. Bandwidth can be checked by sending a large file over the network using a utility program that employs the File Transfer Protocol (FTP). These products are publicly available. You can also use performance tools that are available on some websites. The “Useful Websites” listing at the end of this chapter contains a link to such a site.

Problems never seem to be resolved fast enough. In order to make sure that the dealership has an acceptable level of service, the SLA should detail when service is available as well as how quickly response is expected. This is especially critical with telephone circuits, because a physical repair may be required to solve the problem. Consideration should be given to the need for support on the weekends or late at night. A Standard SLA offers daytime/workweek coverage. Business-level offerings can add later hours and weekend coverage. If charges are incurred for problems after hours, the charges should be noted. If necessary, full 24/7 coverage can be obtained.

All guarantees made must be measurable and monitoring the service will verify that guaranteed service levels are being obtained. Carriers should be asked to provide statistical reports on a regular basis to quantify their performance. The SLA should also detail the penalties that can be imposed on the provider if the service is not delivered as expected. Generally, these penalties are limited to credits applied to the account with the carrier or service provider.

13.3. DETAILED METHODS REVIEW

All access methods are grouped into two categories: wired and non-wired. Wired methods can be broken down further as dedicated line and non-dedicated line.

13.3.1. Wired Methods

Dedicated Line – Wired Method

A dedicated line is a telecommunications path between two points that is available 24 hours a day for use at those sites. It may be either a physical cable or a logically switched system. Therefore, the network speed is guaranteed and predictable. Unlike dial-up these lines are not shared. A dedicated line can be a physical path owned by the dealership or rented from a telephone company, in which case it is called a “leased line”. Examples of dedicated circuits include Digital Subscriber Line (DSL) and T-1 lines.

Non-Dedicated Line – Wired Method

A non-dedicated line is always shared among multiple sites. When referring to telephone circuits, it can be called a switched line. Sites share a fixed bandwidth while they are connected to the network. Consequently, the network speed is not guaranteed or predictable. Examples of non-dedicated circuits include dial-up lines and cable modems.

The nature of the line, dedicated or non-dedicated, only indicates if a fixed network bandwidth is reserved for the line. Either type of line still has the ability to access the Internet through public or private network infrastructures. Another way of looking at the differences in service would be to consider an example of electrical power delivery. If service is dedicated, it would provide a private power line running from the power plant directly to the dealership. All of the wattage that left the plant would arrive at the dealership. A non-dedicated service would have large wattage circuits starting at the plant and then divided throughout the city until they finally reached the dealership. Most of the time no difference between the

services exist. However, when the dealership and neighboring businesses all put their air conditioners on high, power usage soars and the wattage available to each diminishes. In extreme cases, this can causes brownouts or even blackouts.

Dial Up – Wired Method

This is the most basic and widely available method to access to the Internet. Dial-up refers to a connection to a telephone system where the lines are shared. If the line is available, a connection is made and if not, a busy signal is received. A dial-up connection is established and maintained for limited time duration and the maximum connection speed is 56Kbps. Circuit and carrier limitations may prevent the modem from operating at full capacity. The equipment required to access the Internet via a dial-up line is a regular telephone line and a modem as well as an account from an Internet Service Provider (ISP). . The account should be a business-oriented account that will allow use with generic browser software. Services like AOL or EarthLink often require the use of special client software. Some providers require that access be made through their home page (portal). Both of these requirements can cause application performance and functionality problems.

To enhance the dial-up network throughput, the aggregated dial-up technology has been created. Sometimes referred to as line bonding, this “bandwidth-on-demand” technology combines two or more telephone lines into a single network connection. Manufacturers advertise that a maximum data rate of 230Kbps can be achieved. In areas where DSL is available, work is being done to bond multiple DSL circuits at even higher throughput. The major drawback is that some ISP‘s do not support this technology. If they do, the fee is usually higher as well. Newer products claim that the technology is not dependent upon the ISP and that, other than granting multiple accounts; the multiple connections are transparent to the ISP.

Table 13.1. Dial-up Internet Access

Key Factors of Dial-up		
Costs (Approx.)	Equipment/Install	56Kbps modems are under $100 and are often included with new PC’s.
	Circuit	Uses regular telephone line (at a cost of approx. $50/ month). Multiple lines needed for larger dealers.
	Usage Fees	$15 –$50/month for unlimited access. Call to ISP may be a toll call in some areas.
Terms	Commitment Required	Usually just one month.
	Quality of Service	Most often not guaranteed, but can be lower depending on time of day.
Bandwidth	Capacity	Up to 56Kbps. Circuit and carrier limitations may prevent operating at the full capacity of the modem.
	Consistency	Good once established.
	Latency (Delay)	Initial time to connect can be lengthy or may require multiple attempts. ISP may drop the connection if the line is inactive for a period.
Availability		Generally good across Canada, Mexico, and U.S.

Key Factors of Dial-up		
Installation	Complexity	Dial-up is simple. Average users install it themselves. Aggregate dial-up is more complex and it may require professional installation.
	Support for Business Use	Support is built around standard installations on a single PC; support for business users is only as good as it is for any other user. Some ISPs may not support aggregate dial-up.
Life Span		Very good. Economics will keep alive.
Reuse	Combination Possibilities	Can be used for voice when not connected.

Integrated Services Digital Network (ISDN) – Wired Method

ISDN is a standard for digital transmission over ordinary telephone copper wire as well as over other media. ISDN is generally available from the telephone company in most urban areas in Canada and the United States as well as the major cities in Mexico. In concept, this is the integration of both analog or voice data together with digital data over the same network.

There are two levels of service: the Basic Rate Interface (BRI) intended for the home and the small enterprise, and the Primary Rate Interface (PRI), for larger businesses. Both rates include a number of B (bearer) channels and a D (delta) channel. The B channels carry data, voice, and other services. The D channel carries control and signaling information. The Basic Rate Interface consists of two 64Kbps B channels and one 16Kbps D channel. Thus, a Basic Rate user can have 64Kbps or 128Kbps service.

The Primary Rate consists of 23 B channels and one 64Kbps D channel. A portion of the B channels can be combined in any number to provide data capacity approaching 1.5Mbps. The remaining channels can be set aside for voice traffic. This arraignment can be a very attractive cost alternative to traditional voice service. In some cases, the money saved over traditional telephone costs will more than pay for the cost of the entire circuit.

The primary use for ISDN is for backup, rather than primary Internet connections. With the price of the dedicated T-1 circuits coming down and with some companies charging by the minute where ISDN is being used, T-1 technology is surpassing ISDN as the main Internet connection choice.

Table 13.2. ISDN Internet Access

Key Factors of ISDN		
Costs (Approx.)	Equipment/Install	Equipment usually carrier provided. Install fees average $100.
	Circuit	BRI: $50 / month; PRI: $500 - $1,000 / month.
	Usage Fees	Unlimited hours. You may incur local and/or toll charges. Less expensive plans may be offered, with charges up to $4/ hour after minimum hours. ISP fees for BRI service average an additional $50 – $100/ month. PRI service averages $100 - $1,000 /month.
Terms	Commitment Required	Monthly. Price breaks for longer terms are available.

Key Factors of ISDN		
	Quality of Service	The carrier will guarantee service level.
Bandwidth	Capacity	BRI service offers 64Kbps or 128Kbps with no expansion beyond that. PRI service can offer up to 1.5Mbps capacity.
	Consistency	Very good once established.
	Latency (Delay)	Initial time to connect can be lengthy or may require multiple attempts. ISP may drop the connection if the line is inactive for period.
Availability		Major markets in Canada, Mexico, and the U.S.
Installation	Complexity	Professional installation required for both the circuit and the router.
	Support for Business Use	BRI is designed for use in small business. Demanding customers may find support insufficient.
Life Span		Uncertain. Many users are switching to xDSL where available.
Reuse	Combination Possibilities	In businesses with more than 15 telephone lines, combining voice and data on a PRI circuit can easily be cost justified.

Frame Relay –Wired Method

Frame relay service is designed for high-performance data transmission of traffic between local area networks (LANs) and between end points in a wide area network (WAN). Frame relay puts data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the end points, which speeds up overall data transmission. Since the incidence of error in digital networks is extraordinarily small, error correction is not a problem. For most services, the network provides a permanent virtual circuit (PVC), which means that the customer sees a continuous, dedicated connection without having to pay for a full-time leased line. The service provider determines the route each frame travels to its destination and can charge based on usage. An enterprise can select a level of service quality –prioritizing some frames and making others less important. Frame relay service is offered by all telephone carriers and is supported by the larger service providers. Fractional or full circuits provide service that can range in capacity from 64Kbps to 1.5Mbps.

Table 13.3. Frame Relay Inernet Access

Key Factors of Frame Relay		
Costs (Approx.)	Equipment/Install	Average $1,000. Many carriers will waive install fees
	Circuit	$200 – $500/month based on capacity
	Usage Fees	ISP will charge $100 – $1,000/month based on capacity
Terms	Commitment Required	Usually one-year minimum
	Quality of Service	Carrier engineers circuit to the installation. Level of service are guaranteed

Key Factors of Frame Relay		
Bandwidth	Capacity	64Kbps minimum with expansion up to 1.5Mbps
	Consistency	Circuit is shared, so results can vary slightly. Carrier will guarantee minimums and maximums
	Latency (Delay)	Circuit is shared so results will vary slightly. Carrier will guarantee maximum
Availability		Excellent in Canada, Mexico, and the U.S
Installation	Complexity	Professional installation required for both the circuit and the router
	Support for Business Use	Because of the wide range of bandwidths, solutions for dealerships of any size can be found
Life Span		Many users are switching to xDSL where available, but carriers are committed to offerings. Prices are dropping to compete where xDSL is available
Reuse	Combination Possibilities	It is not ideally suited for voice or video transmission, each of which requires a steady flow of transmissions

T-1 - Wired Method

A T-1 line is a dedicated connection consisting of up to 24 channels - each having 64Kbps of capacity. A full T-1 uses all 24 channels to provide 1.5Mbps of capacity. A fractional T-1 uses any number of channels up to 24. One channel will provide 64Kbps of capacity. Two channels provide 128Kbps; and so on. T-1 and frame relay circuits are similar, however frame relay traffic is shared among multiple locations. Generally a T-1 line has better performance and is more reliable than a frame relay circuit. A T-1 line can also be set up to carry both voice and data, thereby reducing the number of voice lines in the dealership. This can help to justify the expense of a T-1.

Table 13.4. T-1 Internet Access

Key Factors of T-1		
Costs (Approx.)	Equipment/Install	Average $1,000
	Circuit	From $300 - $500/month. Pricing may be distance related
	Usage Fees	ISP will charge $100 – $1,000/month based on capacity and distance
Terms	Commitment Required	Usually one-year minimum
	Quality of Service	Level of service will be guaranteed
Bandwidth	Capacity	128Kbps to 1.5Mbps
	Consistency	Excellent. Carrier will guarantee performance
	Latency (Delay)	Excellent. Carrier will guarantee performance
Availability		Excellent in Canada, Mexico, and the U.S

Key Factors of T-1		
Installation	Complexity	Professional installation required for both the circuit and the router
	Support for Business Use	Because of the wide range of bandwidths, solutions for dealerships of any size can be found
Life Span		Good. Only generic technology that offers this much bandwidth
Reuse	Combination Possibilities	In businesses with more than a dozen telephone lines, combining voice and data on a circuit may easily be cost justified

Cable Modem - Wired Method

Recently many cable companies have recognized the need for high-speed access to the Internet, and the distinct advantage they have in providing this service. Because cable companies already have a high-speed connection to many homes and businesses in the form of cable TV, they are able to rapidly deploy high-speed data communications by taking advantage of this existing cable infrastructure. Where available, cable customers simply order the service and a technician comes out to install a modem designed specifically for cable access to the Internet. The cable modem is a device that connects a local area network to a cable TV line.

Like many cable TV receivers, cable modems are typically part of the Internet cable access and are not purchased and installed by the subscriber. Typically, the cable modem attaches to a standard 10Base-T Ethernet (network) card in the computer by a RJ-45 plug (standard network jack) and attaches to the cable wall outlet using a coaxial cable line.

At top speeds Cable Internet access can download data from 2 to 5 Mbps, with typical rates of speed at 500kbps to 1Mbps. The upload speed is also very high but generally much lower than download rates. Usually uploads speeds range from 128Kbps to 500Kbps. These speeds are comparable with large telephone circuits, yet these speeds are subject to availability, and levels of service provided by the local cable company. Due to its high speed and comparatively low cost, cable modem access to the Internet may appear to be an attractive option.

With these advantages, cable Internet access also comes with some significant downsides, especially for a business. There are a number of challenges faced by the cable industry, including return-path capabilities, customer service issues and standards. Cable modems use “shared” bandwidth for multiple subscribers. This means that unlike the dedicated amount of bandwidth obtained with a telephone circuit, cable bandwidth is divided among numerous other Internet subscribers. Subscribers have reported that performance can vary and, at times, is reduced to that of a standard dial-up modem. While this is an extreme situation, it can be expected that the network performance will deteriorate as local usage increases during peak Internet traffic periods. For example, when many people return home from school or work and begin to use the Internet, during the afternoon and early evening, network performance will degrade. This probably coincides with the peak usage in the dealership as well, compounding the problem. If a cable connection is chosen for a business grade service, make sure that an SLA is available from the provider.

Table 13.5. Cable Modem Internet Access

Key Factors of Cable Modems		
Costs (Approx.)	Equipment/Install	Included (standard modems without business-class features).
	Circuit	$150/month for business grade
	Usage Fees	None
Terms	Commitment Required	Monthly
	Quality of Service	Service Level Agreement may not match business requirements.
Bandwidth	Capacity	Variable capacity is offered up and downstream. Usually 128Kbps upstream and up to 5Mbps downstream.
	Consistency	Very sporadic. Performance will drop during peak usage hours in afternoon and evenings.
	Latency (Delay)	Very good but it varies with peak load.
Availability		Limited to parts of major markets in Canada and U.S.
Installation	Complexity	Professional installation required for both the circuit and the router.
	Support for Business Use	Business grade service may not be available from all providers.
Life Span		Emerging technology. Cable and telephone industries merging.
Reuse	Combination Possibilities	Limited. Cable TV can be used in waiting rooms, lounges, etc.
Other		Concern over security since the LAN is part of larger cable company WAN.

Cable companies tend to market Internet access only to home users. Information is publicly available on methods of attaching cable modems to a LAN. The real roadblock is the level of support from the provider. Cable access targeted for home use does not include the same level of service as offerings designed specifically for a small business. In fact, many cable service providers have a policy against using their service for business access. This should be thoroughly investigated before subscribing to any cable Internet service for business use. If the cable provider has a business services group, talk to them directly to get questions answered. Make sure the Service Level Agreement offered by the cable provider does not prohibit the use of their service for business purposes.

For some business purposes, the concept of a fixed IP or static IP may need to be implemented. This allows for the same external IP address on the cable modem to be maintained at all times. This would be necessary if an external vendor would need to connect to the device for any on-going business needs.

Fiber Optic - Wired Method

In the past few years Fiber Optic Internet access has become more available and affordable for consumers and businesses. This internet access method provides speeds varying from 2 MBPS and up to 1 GBPS. The increasing number of service providers, makes this access method a better alternative to cable, especially if scalibality is a concern.

Although this looks good on paper, there are a few key aspects that one should consider before taking this route. Availabilty is not as good as cable yet, or other broadband access methods; some providers use a mixed of fiber optic and copper cable which creates "bottlenecks" during data transportation, and finally the cost of fiber optic internet access could be higher than other methods.

On the other hand, some of the advantages are: Download and Uploads speeds are usually the same in contrast with cable where the upload spees is considerably lower, bandwidth is very high depending on the service provider.

Table 13.6. Fiber Optic Internet Access

Key Factors o Fiber Optic		
Costs (Approx.)	Equipment/Install	Usually Included .
	Circuit	It starts at about $80.00 USD/month for business grade
	Usage Fees	None
Terms	Commitment Required	Monthly at least
	Quality of Service	Service Level Agreement may not match business requirements.
Bandwidth	Capacity	Variable capacity is offered. Up and down streams are higher than cable. 2mbps to 1gbps.
	Consistency	Very good. Depends on service provider
	Latency (Delay)	Very good but it varies with peak load.
Availability		Limited to parts of major markets in Canada and U.S.
Installation	Complexity	Professional installation required for both the circuit and the router.
	Support for Business Use	Business grade service may not be available from all providers.
Life Span		Emerging technology.
Reuse	Combination Possibilities	Business telephone service.
Other		Concern over security since the LAN is part of larger cable company WAN.

The factors in the table above are based on the current state of this technology. It is expected that these factors can change rapidly, due to other influences such as advancement in technology, and competition between providers.

Digital Subscriber Line (xDSL) – Wired Method

DSL is a technology for bringing high-bandwidth information to homes and businesses over copper telephone lines. xDSL refers to different variations of DSL, such as Asymmetric Digital Subscriber Line (ADSL), ISDN Digital Subscriber Line (ISDL) , Symmetric Digital Subscriber Line (SDSL), High bit-rate Digital Subscriber Line (HDSL) , and Rate Adaptive Digital Subscriber Line (RADSL). The distance between the dealership and the telephone company's central office affects service level and availability. DSL offers rates up to 6.1 Mbps (millions of bits) (of a theoretical 8.448Mbps), enabling continuous transmission of full-motion video, audio, and even 3-D effects. More typically, individual connections will provide up to 1.5Mbps to the dealership (downstream) and about 128Kbps from the dealership (upstream). In theory, one DSL line can carry both data and voice signals simultaneously, although deployment of this technology is limited.

DSL has been targeted to replace older technologies and to compete with the cable modem in bringing multimedia and 3-D to homes and small businesses. In markets where DSL is available, costs for older technologies are dropping to stay competitive. Suppliers claim that eventually as much as 80% of the U.S. population will be able to obtain DSL service. However, the OEM's have determined that less than 25% of dealerships can currently obtain DSL connections. Financial, technical, bureaucratic, and political obstacles have hampered deployment of DSL.

Due to recent bankruptcy filings by DSL providers, dealers should select providers that are financially stable. The failure of several large national DSL providers left large numbers of dealers without Internet service. These dealers have been forced to find new providers on short notice.

Coordination between the local exchange carrier (LEC's) and ISP providers has also been a problem. ISPs are dependent upon LEC's to provide physical circuits and to communicate that availability. LEC's have generally stalled that process in order to keep the circuits for themselves and to protect services like frame relay, which are high-margin product offerings for their operations. Recent Federal Communication Commission (FCC) rulings should help speed that process. Availability of service may be determined by going to www.dslreports.com/prequal. This website is an independently run site that will query the major DSL providers and determine if the dealership location meets the requirements and if service is offered in the area. A positive answer may not be the final word here. Actual availability can only be determined by ordering the circuit. That will cause the providers to measure (called a loop test) the quality of the circuit to verify that DSL service can be provided.

This document will only describe the three most commonly available types of DSL: ADSL, IDSL, and SDSL. Sometimes these are confused with residential-class and business-class product offerings. Some ISPs may even package them that way. Actually, the class of service has less to do with the type of product offered and more to do with the support levels promised and with circuit configuration. Business-level offerings will have a higher quality of service guarantee and they can offer amenities such as a static Internet address, extra email accounts and web server storage. Residential service offers few or no quality-of-service promises and, oftentimes, response to line outages are not handled any faster than those for home telephone circuits. Subscribers have reported circuits that are down as much as 5% of the time. Agreements for residential-class service should be entered into very carefully. Pricing is low and, at times, performance can be very good. However, the low quality of service makes using a residential service a risky business tool. Network performance is affected by the subscription rate. The subscription rate is the number of DSL lines assigned to the CO interface. Carriers refer to that interface as the Digital Subscriber Line Access Multiplexer (DSLAM). The greater the number of customers who share the bandwidth upstream from the DSLAM, the higher the subscription rate is. This means that the network speed can vary and it is not always predictable. Generally, business-level offerings have lower subscription rates than residential offerings.

For some business purposes, the concept of a fixed IP or static IP may need to be implemented. This allows for the same external IP address on the DSL modem to be maintained at all times. This would be necessary if an external vendor would need to connect to the device for any on-going business needs.

In addition, with cable modems, an SLA should be implemented with the DSL provider. This agreement will help in maintaining your business needs as well as your internet connections.

ADSL – Wired Method

Asymmetric Digital Subscriber Line is most often targeted to home and small-business users. ADSL is called “asymmetric” because most of its two-way or duplex bandwidth is devoted to the downstream direction, sending data to the user. Only a small portion of bandwidth is available for upstream or user-interaction messages. This is typically not a problem for web browsing since more bandwidth is required to send web pages down to the user than is required when the user requests the pages. Although greater capacity is available in theory, ADSL service providers in the U.S. often only provide a maximum of 768Kbps downstream and 128Kbps upstream. This is usually done to accommodate subscription levels at the DSLAM.

ADSL is the least expensive (bandwidth/cost) DSL offering. However, support levels for lower-priced offerings are designed for home users. Support may be limited and is not intended for businesses running mission-critical operations. When choosing an ADSL product, make sure to get a business-class Service Level Agreement.

IDSL – Wired Method

ISDN Digital Subscriber Line provides DSL technology over ISDN circuits. Since it requires an ISDN circuit and the speed of the line is about the same, the obvious question is why use an IDSL connection instead of a plain ISDN circuit. The largest benefit of IDSL is that it supports customers located outside the normal distance limitations from the telephone CO. Using IDSL provides the added benefit of having an always-on connection. This eliminates call set-up delays and allows for inbound access. Additionally, a flat-rate billing plan is used instead of per-minute usage fees.

Since both an ISDN circuit and DSL service are required, costs are higher than they would be for either service alone. There also is no natural migration to other DSL services should more bandwidth be required later. That makes IDSL unattractive in areas where other DSL options are available now. However, for users located outside of SDSL or ADSL coverage areas, IDSL may be an alternative.

SDSL – Wired Method

Symmetric Digital Subscriber Line provides equal data transmission rates in both downstream and upstream directions. ISPs normally provide better Service Level Agreements with SDSL offerings than are available with ADSL or IDSL. Additionally, the guaranteed transmission rates are normally higher.

Table 13.7. xDSL Service Comparisons

DSL Type	Description	Data Transmission Rate	Distance Limit (not supported by all providers
ADSL	Asymmetric Digital Subscriber Line (ADSL)	768Kbps-6.1Mbps downstream	18,000 ft (1.5Mbps)

DSL Type	Description	Data Transmission Rate	Distance Limit (not supported by all providers
		128Kbps-604Kbps upstream	16,000ft (2.0Mbps)
			12,000ft (6.3Mbps)
			9,000ft (8.5Mbps)
IDSL	Digital Subscriber Line (ISDL)	144Kbps duplex	50,000 ft
SDSL	Symmetric Digital Subscriber Line (SDSL)	128Kbps-1.5Mbps duplex	18,000 ft (24-guage)
			12,000 ft (26-guage)

Table 13.8. xDSL Internet Access

Key Factors of xDSL		
Costs (Approx.)	Equipment/Install	Often included, but some carriers can charge up to $350
	Circuit	ADSL: $50 – $100/Month, IDSL: $90 – $160/ Month ,ISDSL: $100 – $400/Month
	Usage Fees	Usually none. Plans offer unlimited (or very high) usage limits. Check plan carefully
Terms	Commitment Required	Monthly
	Quality of Service	Since it is targeted at business customers, SDSL often has better Service Level Agreement terms. ADSL and IDSL usually offer lower service levels
Bandwidth	Capacity	The distance to the central office and the quality of the existing telephone line determines the speed. Maximums are: 768Kbps (ADSL); 144Kbps (IDSL); 1.5Mbps (SDSL)
	Consistency	Since access at the CO is shared, speed can vary greatly, especially at peak times. Performance is at the mercy of the subscription rate at the DSLAM. Business-class offerings will offer better consistency in part due to lower subscription rates ADSL: Only maximum bandwidths are guaranteed – not the minimum IDSL: The downstream and upstream bandwidths are guaranteed SDSL: The downstream and upstream bandwidths are guaranteed
	Latency (Delay)	Minimal latency: Always on connection
Availability		Limited to major markets in the United States and Canada. Less than 25% of dealers have coverage today. Circuit availability and speed is dependant upon distance for the CO

Key Factors of xDSL		
Installation	Complexity	ISP MUST arrange for circuit install. Router install and configuration will be dealer's responsibility
	Support for Business Use	DSL lines do not seem to be repaired with the same urgency as commercial (T1) lines
Life Span		Initial growth has slowed. Important offering for telephone companies
Reuse	Combination Possibilities	Voice and data may use the same line simultaneously (ADSL and SDSL only).

13.3.2. Non-Wired Methods

Emerging access methods such as wireless and satellite with enhanced technology may be good alternatives when wired methods are unavailable or are highly priced. New-product announcements in both of these areas promise even greater capacity. Since these products have to compete with wired alternatives in order to be truly successful, suppliers are under pressure to deliver them at the lowest possible price. All of the access methods mentioned so far rely on a physical connection with the telephone company or ISP. Wireless connectivity has recently been emerging as an Internet access alternative.

Satellite Technology –Non-wired Method

Satellite technology could be another alternative to consider for dealerships in locations where other access methods may be unavailable or other wise not practical. The current OEM satellite systems were not designed for Internet access and may need to be upgraded or supplemented with additional equipment to perform this functionality. The greatest limitation of using satellite technology for Internet access is the relatively large amount of latency. Latency is the amount of time it takes for data to travel between the user and the satellite and back down to the central ground station and then back again. Using various techniques including IP spoofing, caching, and compression can reduce this problem.

New companies have devised solutions that deal with the latency problem. Many of these companies require new installation of hardware at each location that is using satellite. These solutions have a large benefit to the latency problem, however the price of these solutions are much higher.

Table 13.9. Satellite Internet Access

Key Factors of Satellite		
Costs (Approx.)	Equipment/Install	Included
	Circuit	N/A
	Usage Fees	$100 - $300 / month
Terms	Commitment Required	1-3 years
	Quality of Service	98% or better
Bandwidth	Capacity	Up to 6 Mbps downstream, Up to 256Kbps upstream, Minimum data rates can be guaranteed. Maximum data rates may vary with traffic load

Key Factors of Satellite		
	Consistency	Geographic location and weather conditions may affect reception
	Latency (Delay)	Higher than other transport methods (1.5 seconds)
Availability		The service is available everywhere in North America. Global coverage is being investigated
Installation	Complexity	Requires professional install for dish and earth station. Configuration of the earth station is required since it acts as router and firewall.
	Support for Business Use	Business class offerings are becoming available now
Life Span		Emerging now. Life span will depend on market acceptance
Reuse	Combination Possibilities	Video and IP multicast services may be added
Other		May be a cost effective alternative for the locations where there is no high-speed Internet access available or where wired access is expensive

13.3.3. Wireless Internet Access

Wireless Internet access is an emerging technology that offers an alternative to traditional wired methods when unavailable or not cost effective. Note that this technology has limited availability.

Developments in the use of wireless Internet access technology are bringing new products to the market. These products offer higher-capacity connections at greater ranges and at lower prices than older wireless products do. Businesses are using these products to provide the “last mile” connection from the Internet to the dealership. The wireless connection is used to get data traffic from the dealership directly to an ISP. In some cases, if the ISP will not support the wireless connection, the wireless signal is terminated to a telephone circuit and then sent to the ISP. Wireless is a good option for connecting multiple dealership sites through a wireless LAN. For more information on wireless LANs see the Wireless Networks chapter.

Another comparable wireless frequency technology is Frequency Hopping Spread Spectrum (FHSS). It operates very similarly to Direct Sequence Spread Spectrum (DSSS). In frequency hopping, the signal hops among a variety of frequencies, with the exact sequence of changes (the hopping sequences) known only to the stations participating in the communication. At any instant in time, the signal is being broadcast on only one frequency and the transmission remains on each frequency for only a short time (up to 0.4 seconds) before moving to the next frequency. Thus, interference on a single frequency, or even several frequencies, is not sufficient to disrupt the communication.

In a 2.4GHz FHSS system, the signal hops the entire band using a pseudo-random sequence. All units in a cell must hop at the same time. Each device hops using the same sequence repeatedly, but the devices must be synchronized. This is accomplished by all units knowing the pattern of hopping, the duration of each hop, and the current time of the hop sequence. To prevent interference, multiple FHSS and DSSS systems should not be installed in the same location.

From the viewpoint of the local area network, use of wireless links is transparent. Traffic travels between sites using the same network protocols that wired alternatives use. An extension of the current standard is being developed to support personal devices like cellular telephones or handheld computers.

Table 13.10. Wireless Technology Comparisons

	FHSS	DSSS
System Focus	Economic Solutions	High-performance solutions.
Cost	Lower-cost wireless components	Higher-cost wireless components. However, total system costs may be less as fewer access points are needed as compared to a similar implementation based on FHSS.
Data Rates	Lower per-node bandwidth – the "over-the-air" data rates are about 50% of DSSS systems.	Higher per-node bandwidth/"over-the-air" data rates. Able to migrate to 11Mbps solutions in the future.
Range	The range is smaller compared to DSSS.	Increased range. More suitable for large coverage areas.
Interference	Very low, as multiple frequencies and channels are being used.	Relatively higher than FHSS as only a single frequency is used.
Scalability	Scale up to 10Mbps by adding more access points (maximum of 8 for 1Mbps).	Absolute limit of three non-overlapping channels.

Table 13.11. Wireless Internet Access

Key Factors of Wireless Access		
Costs (Approx.)	Equipment/Install	$300
	Circuit	$150/Monthly
	Usage Fees	None
Terms	Commitment Required	1 year or more
	Quality of Service	Some guarantees are available. Make sure that SLA covers both wireless transmissions and wired connections from the transmission tower to the Internet.
Bandwidth	Capacity	Up to 11Mbps (with greater capacity expected later). Typical offerings are 1.5Mbps. May differ on upstream and downstream volumes.
	Consistency	Good. Transmissions are unaffected by the weather.
	Latency (Delay)	Good.
Availability		Currently has limited support from ISPs. Range is good, up to 35 miles from a transmission tower. However, a clear line of sight is required between dealership and the tower.
Installation	Complexity	Very complex. Site survey required before install. Professional installation required.

Key Factors of Wireless Access		
	Support for Business Use	Business-class offerings are being announced alongside residential offerings.
Life Span		Emerging now. Market acceptance will determine longevity.
	Reuse	May be possible to combine with limited amount of voice traffic.

13.4. NETWORK TRAFFIC LOAD

What is the impact on network performance as more users are added to the network? Will the connection that is planned for installation now for use by six users handle the addition of 10 more users over the next year? It is not always possible to estimate this accurately. Carriers and ISPs may have some formulas that predict needed bandwidth based on the numbers of users. The nature of Internet usage, dealership processes, and data communication protocols make it difficult to obtain meaningful predications. It is important to consider the maximum number of users that will be using the Internet at any one time (concurrent users). Also, consider whether fixed bandwidth is required. If variable bandwidth is acceptable, base requirements on the peak usage period in the dealership. Once the connection is in use, review its performance on a monthly basis using reports showing average and peak usage provided by the carrier.

Preliminary estimates indicate that dealers will initially need at least 128Kbps of bandwidth. As more applications become available, and as more employees in the dealership use the Internet, the bandwidth requirements will increase. These figures are generalizations based on a study of traffic between dealers and OEM’s only. Individual dealers may have a greater or a lesser need. Bandwidth will have to increase if a significant amount of traffic is present to and from other websites.

Installing a connection now that cannot have its bandwidth adjusted later may not be a wise move. Consider options for increasing and decreasing the bandwidth capability for the connection before ordering the connection. If the connection has little or no growth beyond the bandwidth estimate for the dealership, it probably is not the correct choice.

13.5. EXTENSION OF THE CIRCUIT D-MARC

No matter what type of wired telephone circuit is ordered the Local Exchange Carrier (LEC) is responsible for installing it at the site. Depending on the rules from the LEC, the point of installation can vary greatly. The spot at which the LEC terminates the circuit in the building is referred to as the point of demarcation (D-marc). In most cases, the LEC will terminate the circuit at the Minimum Point of Entry (MPOE) inside the building. Normally existing voice circuits would be located at the same spot. If the circuit needs to be continued into another portion of the building to be located near computer equipment, the wiring must be extended. In cases where the LEC is unwilling to extend that circuit themselves, the dealer or another supplier is responsible to provide that wiring extension. When the circuit is initially ordered, find out where the circuit will be terminated and whether the LEC will extend the circuit. If need be, ar-

range for the extension from another supplier. Waiting until the circuit is installed can cause a delay of several weeks. The circuit will not be usable until the wiring extension is performed.

13.6. RECOMMENDED ACCESS METHODS

Please refer to specific OEM addendum for details.

13.7. COMMUNCATIONS BACKUP

No communications method is perfect. Despite promises made in carrier SLA, connections will go down occasionally. Remedies under SLA's only include fees paid for inoperative circuits. Larger sums of money may be at stake in the form of lost business if the connection is down for an extended time. While most connection outages are very short in duration, a backup for that connection is still a requirement. This backup should be a dialed connection attached to the router. The router should have the intelligence to sense that the primary line is down and automatically activate the backup line. In most cases, the dealership users will not even realize this has happened. Once the router sees the primary circuit working again, it will drop the dialed connection. Care should be taken when setting the router's sensitivity to circuit outages. Connections can drop for a few seconds quite frequently. If the router is too quick, it will dial a new connection when one is not necessary. Each dialed connection increases the backup cost. Likewise, connections being reestablished often come up briefly, go back down, and then come up for good later. If the router is too quick to drop the dialed connection, it will only have to redial the connection right away.

For smaller dealerships whose total bandwidth is not much more than the minimum 128Kbps, a dialed backup providing 56Kbps is sufficient. Dialed connections with lesser bandwidth may work but performance will be noticeably downgraded. Larger dealers that require primary connections well above the 128Kbps minimum may need to explore the use of ISDN, DSL, or dialed backup connections. The greater the bandwidth on the primary connection, the greater the backup bandwidth should be. Again, the dialed connections will work, but the lower capacity is noticeable to users and it will affect their productivity. It is quite common to see installations with dedicated or frame relay service using ISDN backups instead of standard dialed connections. Backup communication connections should be checked at least monthly. Nothing is more frustrating to systems administrators than having their backup plans fail. The whole goal of the backup connection is to function in a crisis. When it does not, the dealership loses productivity and the system administrator looks foolish. This backup configuration can be tested by simply disconnecting the primary connection. Within the set time the router should open the backup connection. Once that has been completed, reconnect the primary connection, and the router should drop the backup connection again after the set time.

In worst-case scenarios, it would be wise to keep a dial-up account that can be used from a single PC in the event that access from the LAN cannot be made through the router. This would be caused by the failure of the primary and the backup connections or, more likely, a hardware failure by the router. This secondary backup method will not perform very well, and it cannot service every dealership user at the same time. However, it will serve well enough to transfer parts orders before the shipping deadline, or car orders before the allocation closes.

13.8. INTERNET ACCESS METHOD SUMMARY

There are several different methods available that allow access to the public Internet. Each has advantages and disadvantages. The number of PC's, cost, availability, as well as the anticipated number of concurrent users, need to be factored into the decision process. While the final decision is the dealerships, a table is provided in Recommended Access Methods section to give some assistance in the selection. In order to avoid installation and connection delays, determine where the chosen access method will be terminated, as this point (demarcation) may need to be extended to a different location in the building.

Along with the primary public Internet access method, a primary backup method (usually connected to the router) with an ISDN or telephone line will allow for the continuation of business, but with an impact on performance. An alternate backup method is highly recommended in case of a major failure, such as a nonfunctional router. A dial-up connection from a stand-alone PC would allow access to the public Internet until the primary or the primary backup solutions are in place. The backup solution should be tested on a regular basis to ensure functionality in the case of a real outage. Since the Internet technology is changing at such a rapid pace, keeping the Internet access method contract to as short a term as possible is highly recommended. A month-to-month contract would be ideal and a two-year contract should be considered the maximum.

Table 13.12. Comparison of Access Methods

Transport	Pro	Con
Dialup	Lower cost	Low speed
ISDN	Ubiquitous	Not scalable
	Cost	Limited speed
Frame Relay	High availability	Not scalable
	High speed	High cost
Cable Modem	High speed	Shared access
	Lower cost	Limited availability
		Generally no business service
Fiber Optic	High speed	Shared access
	Lower cost	Limited availability
DSL	High speed	Limited availability
	Lower cost	Viability of vendors
Satellite	Low cost	High latency
	Ubiquitous	Transmission delay
		Shared access
Wireless	High speed	Limited availability
	Lower cost	Emerging technology

Transport	Pro	Con
		Shared access

13.9. USEFUL WEBSITES

- http://www.lightreading.com
- http://www.cable-modem.net
- http://www.cablemodeminfo.com
- http://www.dslreports.com
- http://www.isps.com
- http://www.roadrunner.com
- http://www.telcoexchange.com
- http://www.telesat.ca

Chapter 14. INTERNET CONTENT FILTERING

Table of Contents

14.1. OVERVIEW

Internet content filtering is just one part of a complete security solution that is necessary to protect a business against Internet risks such as viruses, malicious code and Internet misuse. However, providing access to the Internet brings many capabilities to a dealership including email capabilities for communicating with customers and suppliers, web sites containing information important, if not critical to daily business operations, manufacturer applications, and instant messaging. The challenge is to provide access to the beneficial aspects of the Internet while protecting corporate users and assets from the potential hazards.

Internet content filtering should not be confused with virus protection. Virus) protection is used to stop a virus from being transferred to a user's computer. Internet content filtering is used to restrict a user's access to certain information or their ability to release information outside of the work environment. Internet content filtering screens information leaving the company network as well as information entering the network. Information that a company may identify as warranting filtering often includes confidential company and employee information, discriminating or obscene material. The content restriction may be applied to an entire company, specific groups or individuals.

Many companies are taking steps to monitor and limit network usage by implementing Internet content filtering products. These products can be strictly software or a combination of hardware and software. Typical sites that may be considered for filtering include those that carry illegal copyrighted material, adult content, games and high bandwidth audio and video streams. Restricting access from certain Internet sites poses a challenge due to the sheer number of new sites that appear daily. For that reason, many content filtering vendors constantly update lists that categorize the types of Internet sites. These updates are usually offered as a subscription download service. Filtering products can also provide reports on what type of usage patterns exist in a dealership. By monitoring usage patterns, companies can begin to proactively mitigate the risks and cost of sensitive information losses, bandwidth overload and employee issues.

To complement filtering tools, employees need to understand the importance and benefits of content security. Dealerships should create a written Acceptable Usage Policy (AUP) document. The AUP will help employees to understand how to use network assets. The purpose of an AUP is to encourage employee behavior that will increase network security, limit legal liability, improve employee productivity and maximize network bandwidth. If monitoring is conducted without employee knowledge it could be counterproductive to the very goals it is attempting to achieve. The most benefit will be derived from programs that utilize monitoring tools in conjunction with employee training in the areas of information se-

curity and appropriate uses of company resources. Electronic surveillance laws vary by county, state and country so be sure to consult with a legal advisor before implementing any monitoring program.

Content filters can use a variety of methods to evaluate content. The most common are:

- **Keyword blocking** - Keyword blocking scans requested web pages for words contained in its list of objectionable terms. If a word is encountered, the page is blocked. Over blocking can occur using this technique, which prevents accessing legitimate sites because they contain a word that is blocked.

- **URL site blocking** - The URL typed into the browser designates the location from where a web page loads. URL site blocking can use either include lists or exclude lists. Include lists permit all sites to the web browser except what is included in a filter list. Exclude lists deny all sites to the browser except what is included in a filter list.

Filters can be used to evaluate email content, browser and instant messaging activity. One example is email blocking. Incoming emails are blocked using a scoring system based on certain attributes present in the email and/or based on the sender’s email ID or other system information. Specific filter lists may also be established by administrators or users to block specific emails.

Increasingly, filtering packages are using both site blocking and keyword blocking usually with a Graphic User Interface (GUI) to ease administration.

Additionally, web-rating systems can be built into web sites and browsers by the authors. The system works by rating web sites by content type. A content advisor setting in the web browser can be configured to accept or reject content based on rating levels. The most well known rating system is called the Platform for Internet Content Selection (PICS), developed by the World Wide Web Consortium (W3C). For example, in Microsoft Internet Explorer, ratings can be administered under the Tools Tab / Internet Options / Content Tab / Content Advisor Enable Button. This feature is a standard component of Internet Explorer. Note that participation in web rating systems is voluntary and therefore it is not guaranteed that all sites will have ratings.

14.2. FILTERING METHODS

Content filtering products can use the techniques below to block a request. The filtering may be applied to emails, web content, or downloaded content.

- **Protocol blocking** - Allows blocking of Internet protocols for e-mail, newsgroups, File Transfer Protocol (FTP), chat, instant messaging, streaming content (video and audio) and Peer-to-Peer (P2P) file sharing. While particularly effective, it can result in blocking access to useful content.

- **User blocking** - Products with user blocking allows for blocking not only on a specific computer but also according to the user who is logged in. This technique is sometimes referred to as user level authentication.

- **Time-of-day blocking** - Access permissions can be set to vary by the time of day.

- **Restricting web page features** - Browser options may be set by users to restrict and filter content including:

    - Privacy controls

- Malicious scripts
- Blocking fraudulent digital certificates

There are a number of things that user training can address related to secure Internet usage. These include, but are not limited to:

- Limiting ActiveX and scripting features
- Careful responses to pop-up dialogue boxes
- Ensuring valid site certificates and numerous browser security settings. Information about browser settings can be found in the help menu of the browser.

In addition, more information for Internet Explorer can be found at:

http://www.microsoft.com/windows/ie/default.mspx []

The single most effective step users can take to protect the network is not opening unknown email attachments, even if they are from an email address they recognize. This is the most common method virus writers use to spread their virus.

There are four options for content filtering: Client based software, server based software, stand-alone appliances (hardware) and managed service.

- **Client based software** - Client based software is installed on the workstation that is used to surf the Internet. This software is in addition to web browsers which offer a certain level of content filtering. Software requires separate installation and maintenance for each workstation. Client based software may be used in environments with a limited number of users.
- **Server based software** - Server based software is installed on a host server such as a web server, proxy server, or firewall and is maintained using administrator software. Server based software allows for the central control of an entire network or single subnet with a single installation. Because of cost concerns and the required network infrastructure, server-based software is typically used in mid to large-sized environments.
- **Stand-alone appliance** - Stand-alone appliances are hardware devices that can be installed on a network you wish to filter and monitor. These are generally higher performance solutions because they use dedicated hardware and are optimized for filtering. Appliance solutions can be scaled for deployment in small to large environments.
- **Managed Service** - This solution involves outsourcing a portion or all of a company’s security infrastructure including content filtering. Third-party managed security solutions have been deployed in all environments.

Some Internet Service Providers (ISP’s) provide content filtering as part of a business grade broadband offering. Check your local ISP offerings for more information.

Dedicated content filtering systems can enhance network performance and control bandwidth usage. Content filtering products may also be used in conjunction with firewall port blocking. For more information refer to Dealership Security.

Table 14.1. Content Filtering Method Summary

Solution Method	Recommendation	One Time Cost	Recurring Cost
Client Solution	–Dealership with limited number of workstations	-Software	–Software updates
		-Install and Configure	-Client configuration updates
			-Support contracts
Server Solution	-Medium to Large Dealerships	-Filtering software	-software updates
	-Cost effectiveness depending on number of workstations	-Server software	Support contracts for HW and SW
		-Server hardware	-Server administration
		–Install and configure	
		-Server backup	
		–Client licenses	
Appliance Solution	-All dealerships	-Appliance hardware	-Software updates
	-Cost effectiveness depending on number of workstations	-Install and Configure	-Support contracts
			-Appliance administration
Managed Service (may utilize any or all solutions above)	-All dealerships	-Procure Service	-Potential lease arrangement
	-Cost effectiveness depending on availability of knowledgeable IT staff		-Support contracts and Administration
			-Software updates

14.3. Useful Websites

The following links provide for reference only and it does not imply endorsement of any company or product.

Content Rating

- www.icra.org/
- www.w3.org/PICS/

Security

- www.cert.org/tech_tips/

Sample Usage Policies

- www.itpna.com/Vision/1999/991010%20Computer%20Usage%20Policy%20Sample.htm
- www.panix.com/~barman/wisp/aup.html

Other

- www.w3c.org/
- www.gartner.com/research/focus_areas/asset_48267.jsp (Security and Privacy)
- www.opsec.com/solutions/sec_url_resource_management.html
- www.group1iam.com/
- www.networknews.co.uk/Products/Software/1132532

Chapter 15. SAFEGUARDING CUSTOMER INFORMATION

Table of Contents

15.1. OVERVIEW

There are several laws that affect how dealers handle and share customer information. Laws change from time to time and it is important that the dealership team be vigilant about understanding current and new laws that apply to the dealership.

15.1.1. Gramm-Leach-Bliley Act (GLB)

Dealers should become have implemented the operational requirements of the Gramm-Leach-Bliley Act (GLB) and the Federal Trade Commission's (FTC) privacy rule (Privacy Rule). The latter rule obligates the dealership operations to disclose to their finance, lease and insurance customers how they use and share consumer information. In 2003, the FTC published a new rule that is in addition to, and independent of the Privacy Rule.

It is the FTC's "Standards for Safeguarding Customer Information" (Safeguards Rule) that seeks to protect the financial institutions' customers from identity theft and other harm by requiring financial institutions (including dealers retail businesses) to assess their data and information controls and take steps to protect customer information from misappropriation, alteration and tampering. The Safeguard Rule deals with how dealers protect information about their finance and lease customers, regardless of whether they retain the obligation or sell it to a third party finance company or leaser.

It REQUIRES all dealers to develop, implement and maintain a comprehensive written information security program. It also requires dealers to ensure their affiliates maintain appropriate safeguards, and dealers MUST select and retain service providers that are capable of maintaining appropriate safeguards, for the customer information dealers share with them. Examples of Service providers include Retail System Provider (RSP) vendors providing dealership computer systems, BDC call center services and firms linking dealers with their Internet-based customers.

The new safeguard rule has three primary objectives:

- First, insure the security and confidentiality of the dealership's customer information
- Second, protect against any anticipated threats or hazards to the security and/or integrity of the dealership's customer information

- Third, protect unauthorized access to or use of the dealers’ customer information that could result in substantial harm or inconvenience to any customer

For purposes of the rule, “customer information “means any information about a customer of the dealer, or information the dealership receives about the customer from financial institutions, which can be directly attributed to the customer.

Compliance with Gramm-Leach-Bliley Act and the FTC privacy rule needs to be taken seriously because the penalties for violations can be quite severe. For more information regarding the FTC Privacy rule, auto dealers' frequently asked questions concerning the rule, and the GLB dealership requirements visit the FTC and NADA websites.

15.1.2. Red Flag Rule

With Identity theft on the rise and the need to protect customers from becoming victims, the FTC implemented a new law. The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The programs must have been in place by December 31, 2010, and must provide for the identification, detection, and response to patterns, practices, or specific activities – known as “red flags” – that could indicate customer's identity theft. Descriptions of the program's requirements are available at the NADA and FTC websites.

Dealers are required to comply because of their auto financing activities. So it is imperative that dealers either complete a plan internally or research and work with a reputable third party to investigate, implement and then periodically audit the necessary programs.

15.2. RECOMMENDATIONS

We strongly recommend a review of a detailed guide for dealers as a first step in developing safeguard programs. There are two areas for research, the first guide, "Safeguarding Customer Information," has been developed by NADA and can be ordered from their web site, www.nada.org. It provides guidelines for dealers as they develop and administer an effective program to comply with the Safeguards Rule.

It is also recommended that the dealer reviews all the necessary information located at the FTC website for implementing Red Flag Rules and determining what activities are considered to be Red Flags. NADA has developed a management guide, "FTC Red Flags and Address Discrepancy Rules: Protecting Against Identity Theft," that may be ordered on the NADA website. In addition to researching the legal requirements a dealer should contact vendors they work with and make sure to have a Service Level Agreement (SLA) from them that includes compliance with the Rules.

Because of the seriousness of the GLB Act and the potential for a significant amount of liability from its noncompliance penalties, dealers should consider consulting legal counsel.

Chapter 16. DISASTER RECOVERY AND BUSINESS CONTINUATION

Table of Contents

16.1. OVERVIEW

Creating a backup plan can be a difficult task. However having a backup capability will not do any good if there is no plan to implement and maintain it. This includes ensuring that dealership personnel are fully aware and comfortable with the functions of the plan. It is also important to understand what needs to be protected and how to maintain that information for retrieval when needed. Some of the reasons for Business Continuation and Disaster Recovery are:

- Continued viability of the business
- Ability to rationally choose a plan of action that best fit your dealerships needs
- Recovery of vital operating information

Before you begin your planning you first need to understand the difference between business continuation and disaster recovery.

Disaster recovery - The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs. The RTO is a function of the extent to which the interruption disrupts normal operations and the amount of revenue lost per unit time as a result of the disaster. These factors in turn depend on the affected equipment and application(s). The RTO is measured in seconds, minutes, hours, or days, and is an important consideration in disaster recovery planning (DRP). (whatis.com)

Business Continuation – A Business Continuation plan looks at the immediate and temporary restoration of critical business functions so a company can survive a disaster. A BC plan does not address the complete restoration of a business to its pre-disaster condition. (Mehling)

16.2. RISK ANALYSIS

The main purpose of risk analysis is to help the dealership identify all the areas for which there may be a risk of loss. This can be hardware, software, building, personnel, etc. After the various items have been identified the dealership can identify the level of each risk and determine how that risk affects the dealership.

As with any level of risk the actual loss that is felt is completely determinate on the level of protection that already exists. To understand how to mitigate these and other risks go to the Mitigating Risk section in this chapter

To help identify some of the various categories of risk, below is a list of some of the risks that a dealership may be faced with. Review the list below:

16.2.1. Potential High Impacts

Permanent Data Loss Add to this the information about possible financial impact, extreme measures, etc. This can also be in the med and low risk, depending on the amount and type of data lost.- These items can be extremely costly to a business and could even shut down general business operations. An example of these could be Accounts receivable information or information audit information. If a company does not have the correct money coming in it could effect how they operate going forward.

There are various types of loss in addition to data. Some of these which can cause a high impact are:

- Key Personnel - This could be an employee that has vital information that cannot be replaced easily
- Building - Loss of partial or entire building structures
- Key system failure - This would be a main server that allows for data processing, or possibly a server that contained vital information
- All systems are somehow down.(virus, etc)

16.2.2. Potential Medium level Impacts

(Not a key person, but) Personnel Loss – Cross training and documentation of process will help to reduce downtime if an employee is suddenly no longer available. Another important part of the process is to understand who the key personnel are in getting the business back up and running in the event of a loss.

One example of this risk could occur from having one person carry on the key information during travels and that information gets lost in baggage, etc:

- Re-coverable Data Loss – These items are anything there is a hard copy of that could be re-entered. Although this still could cause time delays the damage is minimized.
- Long term power outages - Long term service repairs that last more then a few hours up to several days, natural disasters, and electrical failure inside the dealership.
- Short term power outages - This can be power surges, service interruptions lasting less than a few hours, or natural causes due to weather, etc.

16.2.3. Potential Low level Impacts

Personnel Loss - Loss of a example may be a data entry clerk. This risk is only considered low level when the person who left does not have critical business knowledge that no one else in the organization has. It is also dependent on how quickly those people's tasks can be migrated to existing persons or replaced by a new person. Some of the potential impacts are:

- Software problems – Such as just the need to re-load the software, this does not affect the data.
- Hardware peripheral – Printer down, monitor down, or mouse and keyboard issues that may take approx 20 minutes to fix, but do not have large impact.

16.3. MITIGATING RISK

16.3.1. On-site

There are various ways that an organization can mitigate risk. These plans or solutions can be either on-site or off-site. On-site would be anything that physically exists on the premise of the dealership. Off-site could be anything from remote back-up of electronic information to a physical storage of information at a warehouse or safety deposit box.

Another factor in the resolution of risk is the amount of time that it takes to recover the information and reduce the impact of the occurrence. Below is a list of just some of the many ways that you can prepare for or recover from a disaster occurrence:

- Hardware Loss – With regard to hardware loss there are several different options to accommodate this depending on the item to be replaced.
- Secondary Server (HOT SWAP) – Having a duplicate server with the exact hardware, software, etc. This would allow the dealer to easily switch to the secondary server without excessive down time. This solution is only useful if the primary data does not reside on that server only. Another solution would be to have duplicate server running and have the data duplicated to it nightly.
- Machine in storage (COLD SWAP) – Having an extra computer/server available on-site. This machine does not have any software loaded so it would take more time to load system information and get the computer up and running. This option only works if there is a plan set in place to get the software and other information installed. A few examples of these may be:
  - Drives
  - Computer Monitors
  - Keyboards
  - Video Cads
- Fire protection - There are many things that you can do to protect your information on-site from fire. However before purchasing a fire-safe it is important to have a plan of the information or content that will be placed in the safe. There are various different types of fire-safes, and many of the lower end

systems do not protect any electronic types of information, this would be CD's, DVD's, etc. Also before purchasing review the average storage information and determine the size needed.

- Software - Another plan to set in place is to back-up software and software keys. Copies can be made of most software CD's, but it must be understood that these cannot be used in addition to the existing software, only as a replacement if the original is lost. In addition to the actual CD there are Software keys, these come with all licensing types of software and should be written down somewhere for safe keeping. Make sure to keep these in a safe place because if these are used without permission the dealership could be liable in an audit.

- Power Protection - With power protection there are various levels of protection, based on the type of disaster. Listed below are a few of the most common types of power protection:

- Uninterruptible power supply (UPS) - A source of power that remains constant during a loss of power. These will last for a designated amount of time and can help reduce damage caused by sudden power loss.

- Surge Protector – An appliance that reduces damage caused by sudden electrical spikes caused by nature or general electrical issues.

- Generators – Used to supply power during an electrical outage. These can be for short term use. NOTE: This will not protect against damage caused by an outage. They will only allow for the restarting and continuance of business.

16.3.2. Off-site

Remote Backup and Disaster Recovery Service

Every dealership is exposed to potential destruction of their computer system by fire, flood, windstorm, etc. With the business operations of the dealership now so inextricably linked to their computer system, the lack of a provision for secure off-site backups and a disaster recovery plan can present a situation where a dealership's operation is severely impacted. Performing complete daily backups of your database is absolutely critical to every dealership.

A "Remote Backup and Disaster Recovery Service" provides disaster recovery and automated daily backup and off-site storage service. The service ensures that your database backups are performed every day, without worry of tape and tape drive problems, and without any manual effort by your employees. An inefficient manual process can lead to missed backups, tape failures, and wasted time and effort.

The advantages of a remote backup and recovery service:

- Personnel time spent administering daily tape backups is no longer necessary

- Daily backups are completely automatic and unattended

- Backup always get done

- Tape and tape drive problems are significantly reduced

- The daily backups are sent offsite to a secure facility, safe from fire, theft, or other hazard

16.4. RECOVERY ADMINISTRATION

16.4.1. Planning

Creating a recovery or continuation plan and where to begin can be the most difficult part of planning. Because business continuation and disaster recovery are quite different, there are different requirements and methods for planning.

Creating a plan does not have to be as difficult. There are several tools, templates and other various services in the market to help a company begin the process and create the plan. To make sure the dealership is prepared, research should be done on the tools available and what best fits the needs of the organization. Before you can implement an effective disaster recovery or business continuation plan there are some questions that need to be asked and few steps that need to be understood. Below is a starting point for evaluating your needs.

- First a team must be assembled. This can consist of outside vendors as well as internal employees of the IT department. It would be beneficial to include representatives from the business departments to help determine their needs.
- Document the critical items that would prevent your business from running. This could be PC access, reporting, etc.
- Research and review various plans available. Check with vendors in your area who provide disaster recovery services

It is recommended that you research the various tools available to assist with creating and completing a disaster recovery or business continuation plan.

16.4.2. Checklist

To begin the process of disaster recovery planning a checklist should be created. This checklist should include items in the dealership that need to be backed-up and rank the importance of each of these items.

For more information about items that should be included in the checklist view the appendix at the end of this document.

16.4.3. Auditing

Having a plan in place is just the beginning of the recovery and continuation process. There are steps that need to be taken to ensure that the plan is effective and that the personnel responsible to implement are prepared. Some of the steps to ensure this are:

- Auditing of the plan to determine it they still meets the needs of the dealerships infrastructure is a vital part of ensuring that the plan will still work.
- To ensure that the plan is effective practice drills should be run on a quarterly basis. These drills need to include all vendors that currently store data or will be affected by the recovery process. After completing the drill run an audit to make sure everything necessary was recovered.

Restoring after the disaster

Restoring is the process of recovering the data or equipment that will allow the organization to be back to full functional as quickly as possible. With restoration it is vital that on at least a quarterly basis the dealership conducts a dry run.

A dry run would run through all of the steps that it would take to restore the information. This would include implementing the plan, gathering the backup information, etc. After the dry run has been completed the team should review any errors, or necessary changes that need to occur.

16.4.4. Backup

More than just having data backed up on a CD somewhere a dealership needs to understand the types of backup and what is right for each of their needs. It may be necessary to have different backup options for different information in the dealership. An example of this would be it may be necessary to backup accounts payable and receivable daily but only back up general document information every other day.

With backups there are two main types of backup available. The following types are:

- Incremental - A "normal" incremental backup will only back up files that have been changed since the last backup of any type. This provides the quickest means of backup, since it only makes copies of files that have not yet been backed up. For instance, following our full backup on Friday, Monday’s tape will contain only those files changed since Friday. Tuesday’s tape contains only those files changed since Monday, and so on. The downside to this is obviously that in order to perform a full restore, you need to restore the last full backup first, followed by each of the subsequent incremental backups to the present day in the correct order. Should any one of these backup copies be damaged (particularly the full backup), the restore will be incomplete.(wikipedia)

- A cumulative backup of all changes made after the last full backup. The advantage to this is the quicker recovery time, requiring only a full backup and the latest differential backup to restore the system. The disadvantage is that for each day elapsed since the last full backup, more data needs to be backed up, especially if a majority of the data has been changed.(wikipedia)

In addition to the types of backup there is also a difference in the amount of data that needs to be backed up:

- Device – example: Imaging of a system

- This can be used once the system is set up to allow for a quick restore or rebuild of an entire system. This can also be used to create a duplicate system layout on a different computer.

- Server/Workstation Batch– export data only on system.

- This method is used when the system software is always intact but there is a need to protect just the data.

When choosing which backup type and frequency to use, it is important to look at the business needs and requirements to determine the best approach to creating a backup plan. The following are a few frequencies that a backup could be conducted:

Data Backup

When considering the necessary items to utilize for an effective disaster recovery backing up data is a key part of this. However there are several different data back up options that are available and many of them are not appropriate for recovery purposes. Before the plan is finalized review the data backup plan and ensure that necessary information is being collected.

Other options to consider when determining the backup strategy is the consideration of utilizing a hosting service. There are many things to consider when utilizing this option:

- What are the backup options, nightly, weekly, etc.,
- Where do they store the information
- How often can you access that data and is there a charge
- What is their disaster recovery plan
- What is their level of support (SLA)

For more details regarding some backup types and their uses review chapter 16.3 preventing data loss.

Software Backup

In addition to backing up data it is important to back software as well. This may be getting copies from the manufacturer or creating CD copies. However it is important to note that copies can only be used in the event of an emergency or loss of the original CD, and a legal CD key must exist.

16.4.5. Legal

Understanding the rules around data protection, transportation and storage. There are several laws around protecting customer data, see chapter 10 Safeguarding Customer information for more details.

As a result the dealership should not allow just anyone to transport back-up CD’s or have primary access to the customer information. A careful log should be kept of each person assigned to transport the information and how that is being conducted. It is also important to audit this procedure as well. Someone may audit that transport by calling or visiting the storage location to verify the contents have been delivered.

Chapter 17. Backups

Table of Contents

17.1. Overview

The practice of backing up data on a regular and timely basis using a reliable medium is critical to the success of a dealership. A loss of data can be costly not just in terms of money, but in terms of time, resources, and critical data that can in some cases be the backbone of a business. Any business working with data must have a backup procedure in place at all times.

The key to implementing an effective backup procedure that meets the dealership's needs is to first understand the key components of a backup:

- The type of backup
- The frequency of the backup
- The type of data and how much of that data to backup
- The type of backup medium to use

17.1.1. Backup Methods

There are four backup methods that can be performed:

Full Backups

A full backup, the most comprehensive of the four backup types, contains the entire contents of a disk, including files and folders that have been selected for backup regardless of when they were last modified. Given that it is a full backup of all data, the time to perform the backup can be time consuming and requires adequate storage space. However, given the improvements in backup media these obstacles can be easily overcome. Although the full backup is more time consuming, it does however lead to speedier data restores.

Given the time it takes to perform a full backup, this backup method is typically relegated to weekly or monthly, and supplemented with daily differential backups.

It is considered a best practice to perform a full backup before any major system changes are performed.

Advantages

- The full backup is the most comprehensive backup method.
- The restore process is significantly faster than with other methods and will provide a more efficient and complete restore.

Disadvantages

- While it is the fastest method to restore, conversely it is the slowest method for backing up.
- The full backup method requires significantly more storage space than other methods of backup due to the amount of data being backed up.

[Backup4All2009]

Incremental Backups

An incremental backup contains only the files that have been modified since a previous backup. In the case of incremental backups, multiple backups are kept. There is an original backup of data that is stored, with all subsequent backups containing only information that has changed since the previous incremental backup. Due to incremental backups only containing data that has been modified, the method is more efficient both in time and storage requirements. If there is no change in the source data then there is no additional storage space being utilized and the backup is faster.

The draw back to the incremental backup can be found in its name. It is only an increment or increments of the full backup. Therefore, to perform a restore of the data requires the most current full backup in addition to all of the incremental backups performed since the that most current full backup was taken. This requires more restore time.

Advantages

- With incremental backups only containing data that has changed, this method is extremely time and space efficient when it comes to performing a backup.

Disadvantages

- While it may be more time efficient when performing a backup, it is considered one of the slower methods for restore.

[Backup4All2009]

[Wikipedia2009]

Differential Backups

A differential backup contains all of the files that have been modified since the last full backup was performed. This is not to be confused with an incremental backup which contains modifications since the last **incremental** backup was performed **not** the last **full** backup. Unlike an incremental backup, a differential is not as time and storage efficient requiring more time to backup and more storage space. In contrast, the differential method is quicker to restore than that of the incremental method.

When compared to a full backup, a differential backup will require less storage space but a longer restore time.

Advantages

- Differential backups provide a quicker restore than that of incremental backups.
- Differentials require less storage space and provider quicker backups than full backups.

Disadvantages

- While differential backups provide a quicker restore than that of incremental backups, the opposite is true when backing up.
- Similarly, while differential backups provide quicker backups than full backups, the opposite is true when restoring.
- Storage space requirements for differential backups are higher than that of incremental backups but less than that of full backups.

[Backup4all2009]

Mirror Backups

While the full backup method is the most comprehensive, the mirror backup method is the fastest. A mirror backup is an exact replication of selected files and folders.

The mirror backup method is similar to the full backup method with two exceptions:

1. Mirror backups do not compress files into an archive. Instead they are keep separate and "mirror" the original backup source files and file structure.
2. Mirror backup files are not password protected.

These two exceptions are what make mirror backups the fastest backup method, however there are also draw backs to the method. The mirror backup method requires a large amount of storage space and version tracking of files is not possible.

Advantages

- Mirror backups are considered the fastest backup method.
- Because the backup is an exact mirror of the original source and not compressed, navigation of and access to files and folders is easier.

Disadvantages

- Unlike full backups, files and folders are not compressed requiring larger amounts of storage space.
- Files and folders are not versioned nor password protected.

17.1.2. What and When to Backup

How often data is backed up depends largely on how frequently the data is changed and the relative importance of the data. Data that is critical and that changes frequently should be backed up more frequent-

ly. For example, critical data that is changed on a daily basis should be backed up nightly . Data that is less critical and changes less frequently can be backed up on a weekly basis.

Regardless of the frequency at which a backup is performed, thought should be given to the scheduling of the backups relative to system usage. Optimal backup times would be when system usage is at its lowest, ideally during off peak hours.

As with frequency, the type of data chosen for backup depends on the importance of the data. Data that is critical, sensitive in nature and irreplacable would need to be backed up.

[MicrosoftTechNet2009]

Backing Up Software

In addition to backing up important data, it is also important to have backup copies of original software applications. When a system is being restored from scratch, all the original software applications must be reinstalled. If the original software media is available, it can be used for the restore. However, in the case of a disaster the original software media may have been destroyed. Therefore, it is critical to have a copy of the installation media on a cd or dvd and stored at an offsite location. Another software backup option is to keep a soft copy of the original software installation files backed up along with the other data that is being periodically backed up. With either option, it is important to maintain a copy of the original product license key. This information will be required upon installation.

One important component that should always be backed up is a system's operating system or "OS". Not only are OS backups vital in complete restores of downed systems from disasters, virsuses, etc., but they can also be useful when systems experience increasing amounts of performance degradation.

17.1.3. Backup Media & Services

When it comes to the media to be used in the backup of data, there are several different options available.

Magnetic Tape

Magnetic tape and tape drives, the device uses for performing the backup to the magnetic tape, is one of the oldest forms of data storage. Magnetic tape is typically packaged in cartridges and cassettes. It is capable of holding larges amounts of data and is less expensive then other backup media such as cds and dvds. Given the amount of available storage space on magnetic tape, it is typically used as a high capacity medium for large computer systems.

Once backups are made to magnetic tapes, the tapes are typically stored off site to guard against loss in the case of a disaster.

[Wikipedia2009]

Disc Imaging

A disk image is a software copy of a physical disk. It saves the entire data from the disk, including the file structure and all files and folders from the disk, in a single file. Because disk images are exact copies, or "clones," of original disks, they can be used to duplicate disks or serve as full backups in case a system restore must be done.*

Some companies use these images to restore information after a system crash while others use them as a maintenance tool. Some of the common uses for disc imaging are:

- Protection of files and data
- Producing working backups to manage the most common types of storage issues (e.g., mistakenly deleted files)
- For use in Disaster Recovery testing and implementation
- Easy testing of software configurations with virtual images
- To ease system administration tasks
- Backing up workstations for restoration or maintenance cleaning

[TechTerms2009]

On-site Hard Drive or Server

An on-site server or "backup server" as it is frequently referred to, is a computer used on the premises within the existing network to store copies from individual as well as other server machines. This machine is typically dedicated to storage only.

[PCMAG2009]

DVD

A DVD is a disc that is used for onsite backups, similar to magnetic tape and tape drives. The information is written to the DVD and is then stored either on or off site.

USB Drive

A USB drive, also known as a flash drive or keychain drive, is a plug-and-play portable storage device that uses flash memory and is lightweight enough to attach to a key chain. Storage capicity for a USB device typically ranges from 512mbs to 2gbs, although storage capacities continue to increase over time.

[SearchStorage2009]

Remote or "Off-Site" Server

Similar to the on-site server, the off-site server is used primarily for backing up data. However, this machine(s) is housed remotely in a separate location from the source of the data. The machine(s) is typically connected to the dealer's network with backups being run in an automated fashion.

Cloud-based Storage

Cloud-based storage, a still evolving storage service, provides both straight forward online storage approaches to full scale archive solutions. An Internet-based backup method, data identified for backup is sent via the web to a set of servers maintained by an outside provider specializing in cloud storage.

[SearchStorageChannel2009]

Risks

The following table weighs the risks factors to be considered when selecting a backup media.

Table 17.1. Backup Media Risk Factors

Risks	Tape Drives	In-place Hard Drives DVD	DVD	Off-site Server	USB Drive	Cloud
Hardware Failure	High	High	High	High	High	Medium
Software Failure	High	High	Medium	High	Medium	Medium
File System Corruption	High	Medium	Medium	High	High	High
Accidental Deletion	High	High	Low	High	High	High
Viruses	Medium	High	Medium	High	High	High
Theft	High	Low	High	Medium	High	Medium
Sabotage	High	Low	High	High	High	Medium

Cost and Lifecycle

In addition to risk factors, cost and lifecycle must also be considered when selecting a backup media. The following is a list of considerations that should be taken into account:

- Initial Cost - The amount it will cost to setup the initial backup process.
- Ongoing Cost - This includes maintenance and purchase of media products such as additional tapes, DVDs or hard drives.
- Scalability - The ability to expand the scale of the service to allow for more backups.
- Automation - How easy is it to configure the backup service to run without a user having to start the process.
- Convenience - How easy is it to retrieve or export the data or backup information.
- Performance - What is the speed of the device or service.
- Auditable - Can the information be accessed easily to perform internal audits of the backups.

The table below offers a rating for each consideration based on each backup media type.

Table 17.2. Backup Media Cost and Lifecycle

Considerations	Tape Drives	In-place Hard Drives DVD	DVD	Off-site Server	USB Drive	Cloud
Initial Cost	Medium	Medium	Low/ Med	Med/ High	Low/ Med	Medium

Considerations	**Tape Drives**	**In-place Hard Drives DVD**	**DVD**	**Off-site Server**	**USB Drive**	**Cloud**
Ongoing Cost	Medium	Low	Medium	Med/ High	Low	Medium
Scalability	High	Low	Medium	High	Low	High
Automation	Low	High	Low	High	Low	High
Convenience	Low/High	High	Low/ High	Medium	Low / Med	High
Accessibility	Low/Med	Medium	Low / Med	Medium	Low/ Med	Medium
Performance	Low/Med	Medium	Med/ High	Med/ High	Medium	Med/ High
Auditability	Low/Med	Medium	Low/ Med	Med	Low/ Med	Medium

Chapter 18. CLOUD COMPUTING AND VIRTUALIZATION

Table of Contents

18.1. Overview

Important emerging trends in Information Technology can be summarized as Service Based paradigm and Virtualization. With “Service Based paradigm” we condense different acronyms such as Service Oriented Architecture (SOA) and the popular concept Cloud Computing that has relevant business implications. “The main enabling technology for cloud computing, is virtualization. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization”(Wikipedia).

18.2. Virtualization

Virtualization, in computing, means to create a virtual version of a device or resource, such as a server, storage device, network, etc. where the “framework” divides the resource into one or more execution environments. Applications and human users are able to interact with the virtual resource as if it were a real single physical resource.

For instance in a traditional environment if you have 12 different applications (such as DMS, e-mail, CRM, workflow management, HR, etc.) you often have 12 different servers, one for each application (to simplify application management and resource management); in a virtualized environment you can have only 1 actual server with 12 virtual machines on it, while each application believes to run on a physical server. Obviously the new server has to be much more powerful than each single server, but definitely less powerful and much cheaper than the sum of the 12 different servers.

In a dealer environment the most relevant areas for virtualization are Server Virtualization and Client Virtualization, both are interesting and assure consistent savings.

18.3. Server Virtualization

Unfortunately the architecture of today’s X86 computers comes from Personal Computer architecture: they are designed to run just one operating system and application at a time. As a result, even small data centers have to deploy many servers, each often operating at just 10 percent to 30 percent of their capacity.

Virtualization software solves the problem by enabling several operating systems and applications to run on one physical server or "host." Each self-contained "virtual machine" is isolated from the others, and uses as much of the host's computing resources as it requires.

The main benefits of Server Virtualization are:

- **IT management simplification and flexibility: the whole infrastructure can be managed with one console, dynamically increasing or decreasing the resources needed (CPU, RAM and Disks), even switching on or off the servers, and planning backups.**
- **Reduction of global hardware costs**
- **Reduction of electricity costs (including air conditioning) and space saving**

Three products support virtualization of Windows and Linux (the most popular operating systems) and their main applications: VmWare (by far the market leader), XEN (an Open source product, initially developed by University of Cambridge Computer Laboratory) and Hyper-V (by Microsoft).

VmWare has developed different products to virtualize the data centers and to manage them, and sell them with different offering criteria, trying to satisfy both large enterprises and very small organizations. Dealers should spend some time to understand which is the best choice for their needs.

For instance vSphere (a data center virtualization product) is sold through the following licenses: Enterprise Plus; Enterprise; Standard; Essential plus; Essential. Each license provides for different types of use and functionality.

Almost all the new applications run on VmWare, for instance, but some old applications might have problems. Therefore before moving or buying an application it's important to check with the software providers if it runs in a virtualized environment.

18.4. Client Virtualization

Client Virtualization, often dubbed Desktop Virtualization, is the concept of separating the logical desktop environment seen by users from the actual machine (normally a PC). Applications and data run on a remote system, with only display, keyboard, and mouse information communicated with the local client device, which may be a traditional PC, a thin client device, or even a mobile device (tablet or smartphone).

There are different possibilities to virtualize the user desktop, a basic classification, based on hardware choice, is:

- **thick client: a traditional PC/ laptop with virtualization software running on board**
- **thin client: practically a dumb terminal (with keyboard and mouse) with just emulation software preloaded (normally running on Linux). "Zero client" is a particularly case of thin client, with no software on board, because the emulation is performed directly by firmware (i.e. the VDI protocol is embedded at hardware level).**
- **mobile client: tablet (or smartphone) with emulation software to access desktop applications (when the tablet is the main device for the job, but some desktop applications are needed).**

The thin client choice is getting more and more popular because of its many advantages: reduced power consumption, central management and increased security, not to mention the fact that they are cheap and simple.

When calculating electricity savings, also the air conditioning has to be considered; in some cases electricity saving alone could justify the replacement of all desktop PCs with thin clients (with an ROI of less than 3 years). Reduced maintenance costs are another advantage.

Centralized management is probably the most interesting possibility offered by thin clients: software updates can be performed instantly, and for instance you can automatically apply profile policies to groups of thin clients with similar configurations and even switch them on and off automatically at a predefined time.

Increased security is another good point, because no virus exists for thin clients and back-up can be managed and performed centrally, at server level. Through desktop virtualization users can only use the system for company needs, because they don't have admin authorization to install software and USB ports can be eliminated or disabled: this improves security

Thick clients are an appropriated choice when a laptop is needed (e.g. when connectivity is not assured or local applications are needed) and benefits of client virtualization (mainly centralized management and back-up) are desirable.

Another possibility is to reuse old PCs as a client. Indeed the hardware requirement for a thin client is very low (e.g. 1 GB RAM and 1 GHz processor), thus making possible the use of the old PCs as "dumb terminal", for instance loading Linux via network (e.g. etherboot). This approach extends the life of old PCs, allowing to delay hardware replacement.

The following table summarizes main pros and cons of the different solutions:

Drivers	Desktop PC (Thick Client)	Laptop (Thick Client)	Thin Client	Mobile Client (e.g. tablet)
Total Cost of Ownership * (purchasing, maintenance, management, electricity, etc.)	+	+	++++	++ (depending on platform)
Mobility (possibility to be used in different places and travelling)	+	+++	+	++++
Security	+	+	+++	+++ (depending on platform)
Central management (possibility to standardize and centralize updates, backup, configuration, switch on/off, etc.)	+	+	++++	+++ (depending on platform)

Where: "+" means "worst , low grade" and "++++" means "best, very high level" *) Note: for TCO (Total Cost of Ownership) "+" means maximum cost, while "++++" is minimum cost.

In some cases different devices can be used by the same person, for instance a Thin client plus a Mobile client (e.g. iPad) when travelling.

18.5. Cloud Computing

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (NIST definition - National Institute of Standards and Technology).

Cloud computing relies on sharing resources to achieve economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of shared and standardized services, exploited with a consumption model.

Accordingly to NIST, the cloud model is composed of three basic service models:

- Software as a Service (SaaS): the capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure.
- Platform as a Service (PaaS): the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.
- Infrastructure as a Service (IaaS): the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

E-mail and CRM are already used by many dealers with a SaaS model. Many DMS providers (such as CDK and R&R) are already offering something similar to a SaaS model for their DMS (almost all the current DMSs are not designed to be “in the cloud”, but have been adapted to be used via internet). The other 2 models, are rarely adopted by dealers with few exceptions (e.g. IaaS for disaster/recovery is an interesting option).

To be really effective cloud computing requires service standardization, it doesn’t matter if officially defined (such as ISO documents) or “de facto” (such as iOS APIs by Apple). Through standardization, interfaces complexity and integration issues are addressed and misunderstandings are minimized.

Unfortunately this is an evolving field; at technical level some standards are emerging, as WSDL (Web Services Description Language), HTTP (Hypertext Transfer Protocol), Jason (JavaScript Object Notation), REST (Representational State Transfer) and HTML5. Unfortunately the semantic level, i.e. defining and standardizing the business objects (e.g. defining a vehicle), is far from being achieved, in spite of STAR efforts within automotive retail business.

When deciding to leverage a SaaS offering, a preliminary analysis of possible integration issues (e.g. integration between DMS and CRM, if supplied by different vendors) and a specific focus on data ownerships and usability (also after contract termination) is recommended.

Normative References

[Backup4All2009] backup4All.com. *Full backup [http://www.backup4all.com/kb/full-backup-116.html]*. 2009.

[Backup4All2009] backup4All.com. *Incremental backup [http://www.backup4all.com/kb/incremental-backup-118.html]*. 2009.

[Wikipedia2009] wikipedia.com. *Incremental backup [http://en.wikipedia.org/wiki/Incremental_backup]*. Nov 9 2009.

[Backup4all2009] backup4all.com. *Differential backup [http://www.backup4all.com/kb/differential-backup-117.html]*. 2009.

[MicrosoftTechNet2009] Microsoft TechNet. *9 Questions You Must Ask Yourself When Planning a Backup Strategy [http://technet.microsoft.com/en-us/magazine/dd767785.aspx]*. 2009.

[Wikipedia2009] Wikipedia. *Magnetic tape data storage [http://en.wikipedia.org/wiki/Magnetic_tape_data_storage]*. Nov 5 2009.

[TechTerms2009] TechTerms.com. *Disk Image [http://www.techterms.com/definition/diskimage]*. Apr 16 2008.

[PCMAG2009] PCMAG.COM. *backup server [http://www.pcmag.com/encyclopedia_term/0,2542,t=backup+server&i=38374,00.asp]*. 2009.

[SearchStorage2009] SearchStorage.com. *USB drive [http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci869057,00.html]*. Apr 6 2007.

[SearchStorageChannel2009] SearchStorageChannel.com. *Cloud storage services options [http://searchstoragechannel.techtarget.com/tip/0,289483,sid98_gci1323444,00.html]*. Jul 31 2008.

[Ref_Software_Piracy_Definition] Business Software Alliance. *What is Software Piracy?http://www.bsa.org/country.aspx*.

[Ref_Software_Piracy_Types] Aladdin. *Types of Software Piracyhttp://www.aladdin.com/hasp/types-of-piracy.aspx*.

[Ref_Software_Piracy_Audit] Internal Auditor. *The high cost of software piracy: organizations that implement an assetmanagement process can curb the risks associated with an adverse software audit http://findarticles.com/p/articles/mi_m4153/is_3_60/ai_103194421/?tag=content;col1*. June 2009. Mark Bigler.

Appendix A. Dealership Needs Assessment

In order to evaluate what the dealership will need, it is necessary to examine the current network infrastructure as well as plan for the near and more distant future. This will allow dealer to reach more informed decisions on which technologies, suppliers, and solutions are best suited for the dealership's needs.

After filling in this worksheet, the dealer will have the proper information to determine the most efficient and cost-effective solutions for both the short and the long term. Please fill in the appropriate blanks throughout this document as completely as possible.

Network (LAN and WAN)

The dealership network is typically comprised of computer/server room, wiring, wiring closets, servers, Personal Computers (PC's), and connection devices (hubs, switches, routers, etc.). Each of these should be reviewed when assessing the dealerships needs. The more information gathered ahead of time, the better equipped the dealer will be. Provide copies of any schematics or drawings if possible.

Primary and Alternate Project Leaders

The Primary and Alternate Project Leaders will be the main contacts at the dealership. They will be able to coordinate all activities associated with planning , installation , and ultimately , general upkeep of all communication equipment. Ideally , they will have a thorough knowledge of existing dealership systems and future facility and equipment plans and should be available during normal business hours.

Table A.1. Dealership Information

Dealership Name:	
Address:	
City, State Zip:	
Unique Dealer ID:	
Phone Number:	
Fax Number:	
DMS Provider:	
Customer #:	
DMS Name/Model Number:	

Table A.2. Dealership Project Leaders

Project Lead			
Name:		Position:	
Phone Number:		Email Address:	

Project Lead			
Mobile Number:		Fax Number:	
Alernate Project Leader			
Name:		Position:	
Phone Number:		Email Address:	
Mobile Number:		Fax Number:	

Telephone Information

In many dealerships, dial-up connections are used to access OEM websites and other sites during normal business hours. These dialup accounts, telephone lines, and modems have a potential to be replaced by a high-speed Internet connection, which could reduce costs.

Does the dealership have a Private Branch Exchange (PBX)? Yes_____No_____

How many telephone closets exist? _____

How many telephone extensions does the dealership have off the main line? _____

Number of direct lines._____

Number of dedicates fax lines._____

Number of dedicated dial-up Internet lines being used._____

Total number of shared lines (i.e., voice/internet)_____

When does the existing telecommunications contract expire?___/___/____

Existing Documentation

Is there any network documentation such as network designs of existing infrastructure that was provided by an Internet, dealer Management System (DMS), or network service provider? Yes____No____

Can a copy of this documentation be provided? Yes____ No____

If this is a multi-franchised dealership, does the dealer have any network documentation, such as network designs of other OEM infrastructure within the dealership? Yes____ No____

Are there any “green screen” terminals that are connected to a dealer management system or other server systems within the dealership? Yes____ No____

DMS Information

Machine Type? Server____DMS____

Host Processor? Server____DMS____

Operating System (OS)? Server____DMS____

DMS Software Release_____

Features Release_____

Is the DMS server Ethernet Ready? Yes____No___

Does the DMS require Domain Name Server (DNS)? Yes____No____

If so, how will DNS be handled on the dealership LAN? Yes____No____

How will the DMS be handled in a Dynamic Host Configuration Protocol (DHCP) environment?

_____

What is the IP address of the DMS Server? _____._____._____.

What are the IP addresses of any DMS terminal servers?_____._____._____/_____._____._____/_____._____._____/_____._____,_____

What are the IP addresses of any DMS Print servers?_____._____._____/_____._____._____/_____._____._____/_____._____,_____

What are the IP addresses of any other DMS devices?_____._____._____/_____._____._____/_____._____._____/_____._____,_____

How will static IP's for Servers, Printers, and other network devices be handled?

_____

How will static IP's for Servers, Printers, and other network devices be handled?

_____

How many ports are available on the dealership Ethernet switch?_____

How many network printers' connections are available?_____

How many DMS terminals (green screens) are in the dealership?_____

How many terminals will be replaces by Personal Computers (PC's)?

Will additional clients be added to access the DMS? Yes____No____

Does the dealership have multiple locations? Yes____No____

What DMS peripheral devices will work on the dealership network?

_____

Identify how the DNS will be handled on the dealership network.

_____

Identify how the Dynamic Host Configuration Protocol will be handled with the DMS

_____

Will additional clients be added to access the DMS? Yes____No____

When does the existing DMS contract expire?_____/_____/_____

Network Hardware

When planning the need for Ethernet ports, consider wall jacks and ports in hubs and switches. Remember that network printers usually require their own Ethernet ports. Certain areas of the business contain junction boxes for multiple cable runs from that particular area. These junction boxes are the hubs and/or switches. Please list the details for these devices.

Table A.3. Network Details

Hub or Switch	Brand or Model	Number of Ports fille/ Total	Speed 10Mbps or 100Mbps	Location

Are there any routers on site? Yes____No____

If yes how many?_____

Is there a DMS-provided or Supported LAN within the dealership? Yes____No____

Is there OEM(s) provided or supported LAN within the dealership? Yes____No____

Is yes, which OEM?_____

Are there other Local Area Networks (LAN's) within the dealership? Yes____No____

If yes please explain

_____

Hardware and Browser

List all workstations, which include PC's, green screens, service bay devices and servers at the dealership including the applications in the table below:

Table A.4. Site Information

Type of Workstation	Operating System	Browser Type and Version	Internet Access Method	DMS Access	Internal LAN Y or N			

Type of Workstation	Operating System	Browser Type and Version	Internet Access Method	DMS Access	Internal LAN Y or N			

Printing

You may desire additional: laser, form, dot-matrix or color printers. You should incorporate these plans, as well as any other special printing needs, into this plan even if specific plans to purchase the solution do not yet exist. This will allow for planning and cost-effectiveness when addressing categories like wiring, network connection devices, and computer-room-type equipment and environments.

How many dot-matrix printers are attached to green screens?_____

How many of these attached dot-matrix printers are planned for replacement with networked printers?_____

How many networked laser printers currently exist?_____

How many of these laser printers only use pre-printed forms?_____

How many store blank paper and preprinted forms?_____

How many networked laser printers are planned for the future? _____

How many ink-jet printers (black and white or color) printers exist now?_____

How many of these ink-jet printers are networked?_____

Are there any special printing needs that are currently addressed, or that will need solutions in the future? Explain.

_____

Do you need privacy for printing? (add comment about contract examples)Yes____No____

How secure do you want your printing to be? (Ex: passwords, cover pages, etc.)

_____

Wiring Infrastructure

Describe the wiring within the dealership. Is it copper, fiber, wireless or other?

_____

Was existing data wiring installed according to Category 5 or 5e standards?Yes____No____

Multi-site Connections

Does the dealership have any existing multi-site communication lines?Yes____No____

What company provides that existing multi-site communications?_____

If there are multiple sites, what types of connections exist between them? (Circle all that apply) Modem, Frame Relay, ISDN, DSL, Other

What is the bandwidth for each connection?_____

Internet Services

How many users need access to the Internet?_____

Change ISP question to how long do you plan on staying with the same ISP._____

What company provides the existing Internet communications?_____

What is the Internet access method (circle one)? Dedicated, Frame Relay, DSL, ISDN, Other

What is the bandwidth for each connection?_____

What is the typical monthly cost for Internet services?_____

What is the concerning Internet access?_____

IP Addressing

List all IP address space (Private, Public, Static, Dynamically Assigned, Address Ranges, etc.):
____.____.____/____.____.____/____.____.____/____.____.____/____.____.____/____.____.____/
____.____.____/

Does the dealership have registered IP addresses?Yes____No____

If yes, by who and at what range?

_____

Are any private IP address (non-routable over the Public Internet) used?Yes____No____

If yes, by what range?

_____

How are IP addresses assigned? (Circle all that apply) DHCP, BOOTP, Statically set_____

Identify which devices must remain static if switching to DHCP (OEM server, DMS server, printers, etc…).

_____

Internet Network Security

What type of hardware is used for security (firewall, router, PC, etc…)?

_____

What type of software is used for security (Checkpoint, Axent, etc….)?

_____

Is a network security policy enforced?Yes____No____

Internet Network Management

What hardware platform is used to perform network management?_____

What operating system is used to perform network management?_____

What applications are used to perform network management?

_____

Technical Support

Who provides help desk support for the dealership (i.e., OEM, DMS Provider, independent third party) for the following:

Networks_____

Applications _____

Personal Computers (PC)_____

Who provides the Remote (Central) Support?_____

Who provides the Network Engineering Support?_____

Web Services

Does the dealership have a website?

If yes, what are the URLs?

_____

Does the dealership have any registered domain names?

Are additional domains needed?Yes____No____

Who provides the content of the web page(s)?_____

Who provides the web hosting? _____

Does the dealership need additional website development or hosting services? (Please explain.)

_____

How many hits does the website generate per month?_____

Email Services

Who provides email accounts to the dealership?_____

How many users need access to email?_____

How many email accounts are provided from the Internet provider(s)?_____

Does the dealership need access to newsgroups?Yes____No____

Computer/Server Room

Is there a central wiring closet where all networking equipment and communication lines are located?Yes____No____

Does the dealership have a computer room now?Yes____No____

Is electrical power to the network equipment on isolated circuits?Yes____No____

Is there power protection such as UPS and surge protection on these computer room circuits?Yes____No____

How many amps are supplied to each circuit?_____

How many available outlets are near the networking equipment?_____

If there is no computer room, where is the primary location for network hardware and servers located?

_____

Does this computer room have a controlled climate?Yes____No____

Is the computer room equipment on a raised computer platform floor?Yes____No____

Is the access secured to the computer room?Yes____No____

Wireless Access

Do you plan on utilizing wireless LAN?Yes____No____

Do you plan on utilizing a wireless ISP?Yes____No____

Will your customers be able to access the internet through the wireless connection?Yes____No____

Will you have multiple wireless access points?Yes____No____

Will any of your wireless connections have access to your internal network?Yes____No____

Faxing Services

Do you have network fax capabilities?Yes____No____

Do you have faxes coming inbound?Yes____No____

If yes do these contain sensitive information?Yes____No____

Do you utilize internet based faxing?Yes____No____

Appendix B. Checklists

Table B.1. Client Hardware Requirements

Element	Description	Reference	Frequency
Media player plug-in	Periodically review browser versions and associated media player plug-in. Browser have configuration tools to view the plug-in installed on a particular PC	Chapter 12, *MULTIMEDIA DELIVERY*	Every 6 months
Firewall rule sets	Review Firewall rule sets for appropriate access to Web Sites and Content Delivery Networks. Blocking rule sets can limit access to particular sites or networks.	Chapter 11, *DEALER DESKTOP MANAGEMENT*	
Switched LAN wiring infrastructure	Review internal LAN wiring infrastructure for future upgrade to switched LAN capability. Deployment of a dealer switch LAN reduces the impact of network congestion when bandwidth intensive media is delivered to a desktop application or interactive appliance	Review OEM Specific Addendum for requirements	As Necessary
Desktop Requirments	Review Content Delivery desktop requirements for support of required codec’s or players e.g. MPEG-4 codec using Windows Media Player and other encoding formats for video programming, as well as MP3 for music	Review OEM Specific Addendum for Codec and Player requirements	As Necessary

Table B.2. Multimedia Delivery

Element	Description	Reference	Frequency
PC Specifications	Check PC processor, memory and hard drive specifications meet OEM requirements		Three year lifespan is typical
Server Specifications	Check the PC/Server processor, memory and driver specifications to meet OEM requirements		
PC Procurement	Check OEM or VARs for offerings	OEM Addendum	As Required
UPS/Surge Protector	Use a UPS to eliminate power fluctuations and prolong the lifespan of hardware. Surge protectors control power spikes but do not address low power brownout conditions	OEM Addendum	Review UPS and surge protector warranty coverage
Flat Panel Monitor	Check for digital video interface (DVI) option if using flat panel displays.	OEM Addendum	As Required
Warranty Service	Check for service contracts with a same-day on-site repair option to minimize business interruptions	Check OEM or VAR offering	As Required
Anti-Virus software	Check OEM for offerings	Chapter 11, *DEALER DESKTOP MANAGEMENT*	Yearly subscription renewal is typical and daily software updates are recommended
Browser Software	Used to connect to the Internet and OEM	Chapter 11, *DEALER DESKTOP MANAGEMENT*	Update service packs and security patches as required
Operating System(Windows 2000, XP etc)	Check OEM for supported versions		Update service packs and security patches as required

Table B.3. Dealership Network Infrastructure

Element	Description	Reference	Frequency
Wiring Standards	Critical for reliable LAN operations	Chapter 3, *NETWORK DESIGN FRAMEWORK*	When upgrading dealership IT infrastructure

Element	Description	Reference	Frequency
Wireless LAN	Allows LAN activity without physical wiring	Chapter 6, *WIRELESS NETWORKS*	When upgrading dealership IT infrastructure for wireless support
Design Framework	Provide solid LAN backbone and Internet connection	Chapter 3, *NETWORK DESIGN FRAMEWORK*	When upgrading dealership IT infrastructure
Virtual Local Area Network (VLAN)	To access applications or data from dissimilar LAN segments (dealer, OEM, RSP)	Chapter 5, *PRIVATE AND VIRTUAL PRIVATE NETWORKS*	When upgrading dealership IT infrastructures
Private and Virtual Private Network	Private circuits connecting two or more locations	Chapter 5, *PRIVATE AND VIRTUAL PRIVATE NETWORKS*	When upgrading private network configurations
Multi-Building/Location Network	Leverage common IT functions from multiple buildings and locations	Chapter 2, *TRADITIONAL NETWORK INFRASTRUCTURE*	When consolidating multiple locations
Multi-OEM Environment	Use a network switch to manage traffic	Chapter 2, *TRADITIONAL NETWORK INFRASTRUCTURE*	When upgrading support for OEM or RSP
Web-Caching	Temporary storage of frequently accessed Web sites	Chapter 3, *NETWORK DESIGN FRAMEWORK*	When upgrading Internet connectivity

Table B.4. Internet Access Methods

Element	Description	Reference	Frequency
Dial Up	Internet connectivity that requires a modem and telephone line	OEM Addendum	This should be used for limited internet usage.
ISDN	Internet connectivity that requires a digital modem and a digital telephone line.	OEM Addendum	This should be used for limited internet usage. This connection should be used as a last option.
Frame Relay	Internet connectivity that can be configure for direct internet access or directly to a vendor	OEM Addendum	Can be configured for a small or large amount of internet usage.
Cable Modem	Internet connectivity that is provided by a Cable Company. SLA should be applied for a business connection	OEM Addendum	Can be configured for a small or large amount of internet usage.

Element	Description	Reference	Frequency
DSL	Internet connectivity that is provided by a Telephone Company. SLA should be applied for a business connection	OEM Addendum	Can be configured for a small or large amount of internet usage.
Satellite	Internet connectivity that should be used as a last option only. This solution usually has latency issues.	OEM Addendum	Latency is an issue for small interactive transfers. Should only be used where no other option is available or as a backup connection.
Wireless	Wireless Internet connectivity. Coverage is limited throughout the US	OEM Addendum	Very limited coverage in the US. Requires Line of Site.

Table B.5. Dealership Security

Element	Description	Reference	Frequency
Firewalls	Devices or software that allow or block traffic based on rules	Chapter 7, *DEALERSHIP SECURITY*	This device or software should always be kept up to date with the latest code or software version
Personalized Firewall Software	Software that resides on a PC or laptop to monitor and/or block malicious traffic	Chapter 7, *DEALERSHIP SECURITY*	This device or software should always be kept up to date with the latest code or software version
Demilitarized Zone (DMZ)	A security configuration that separated internet facing devices from the dealership's internal network	Chapter 7, *DEALERSHIP SECURITY*	Security audits should be performed every 6 months to determine if there are any new vulnerabilities or patches.
Proxy Servers	A device that accesses the internet instead of the PC or laptop to provide protection for the dealer's internal LAN	Chapter 7, *DEALERSHIP SECURITY*	Proxy server software should be kept to the current version to keep up to date with the latest security vulnerabilities and patches.
Intrusion Detection Software	Devices or software that monitor and takes action traffic based on rules	Chapter 7, *DEALERSHIP SECURITY*	IDS MUST be updated to the latest version to allow for new security vulnerabilities to be recognized
Anti-Virus Protection	Software that sits on a PC or Servers that moni-	Chapter 7, *DEALERSHIP SECURITY*	Anti-Virus software MUST be kept up to date

Element	Description	Reference	Frequency
	tors files and folders for Viruses		as new viruses are appearing every day
Wireless LAN Security	Wireless security that is implemented to protect the dealer's wireless network.	Chapter 6, *WIRELESS NETWORKS*	Wireless Security should be always maintained to the current standards to ensure the dealer's wireless network is protected
Attack Recovery	A plan to implement if the dealer's security is compromised	Chapter 7, *DEALERSHIP SECURITY*	When any change is implemented in the dealer's network, the plan MUST be updated to address these changes
Policies	Security Policies MUST be written to enforce all security measures in a dealership.	Chapter 7, *DEALERSHIP SECURITY*	When any change is implemented in the dealer's network, the policy MUST be updated to address these changes
Physical Security	Ensure that you have the proper physical security measures in place to protect your information.	Chapter 7, *DEALERSHIP SECURITY*	

Appendix C. Disaster Recovery Checklist

1. Do you understand all the data that needs to be included in a back up and how that data relates to your organization?
2. How is your infrastructure protected? Is there a CPU? Are there off-site servers?
3. Have you included outside parties in your recovery plan? This would be anyone that touches or is affected by a disaster.
4. Do you have easy access to the recovery plan? Do others that need it have access?
5. Do you store your backups off-site? If so do you know how to get them when needed?

Appendix D. Project Checklist

The following will serve as a basis for a project checklist. Items may be added or deleted depending on individual circumstances.

Table D.1.

Tasks		Responsible Party
Determine dealership Requirements		
	Assign technical project leader in the dealership.	dealer
	Complete needs assessment (see information in dealership Needs Assessment Appendix D.	Project Leader
Research/Contact Suppliers		
	CReview OEM Packages.	Project Leader
	Contact possible suppliers (OEM package suppliers, local providers, DMS Provider's, etc.).	Project Leader
Supplier Meetings		
	Review needs analysis with possible suppliers.	Project Leader
	Discuss supplier products and services.	Project Leader
	Review Service Level Agreement (SLA) and contracts.	Project Leader and Dealer
Select Network Designer		
	Choose supplier to create design package.	Project Leader and Dealer
	Participate in site survey.	Project Leader
	Designate central wiring locations (if not already in place).	
Local Area Network Design (or Changes)		
	Create floor plan with needed cable runs and hardware (PC's, printers, etc.) locations.	Network Designer
	Determine best Internet access methods primary and backup connections. Make provisions for connection to the LAN.	Network Designer
	Create Statement of Work for new wiring and LAN configuration (if any).	Network Designer
	Create Bill of Material for new wiring and LAN equipment (if any).	Network Designer
Select LAN/WAN Suppliers		
	Deliver design plans.	Network Designer
	Review plans with potential suppliers.	Project Leader and Dealer
	Deliver detailed quotes matching design plans.	Suppliers
	Review supplier(s) quotes and service offerings.	Project Leader and Dealer

Tasks		Responsible Party
	Make final selection.	Dealer
	Identify supplier project coordinators.	Suppliers
	Set project schedule, milestones, and dependencies.	Project Leader and Suppliers Coordinators

Glossary

*

1000BaseT	IEEE 802.3 physical layer specification for 1000Mbps Ethernet over two pairs of category 5 UTP wire.
100BaseT	IEEE 802.3 physical layer specification for 100Mbps Ethernet over two pairs of category 5 UTP wire.
10Base2	IEEE 802.3 physical-layer specification for 10Mbps ethernet over thin coaxial cable. Commonly referred to as thinnet.
10BaseT	IEEE 802.3 physical-layer specification for 10Mbps Ethernet over two pairs of Category 3, 4, or 5 UTP wire.
110 Block	See Connecting Block.
66 Block	See Connecting Block.

A

Acceptable Usage Policy (AUP)	A document that clearly states what an employee can and cannot do while using the Internet at a dealership. Can contain liability disclosures and actions that could result in termination
Access Point	A wireless hub that uses radio frequency to communicate with other wireless devices.
Addressing	A numbering system, which uniquely identifies computers and devices on a network.
Advanced Network Exchange (ANX)	A VPN originally instituted to allow suppliers and OEM’s in the automotive industry to link their networks. Have now expanded their customer base beyond the auto companies.
Advanced Research Projects Agency (ARPA)	Underwrote the development of the Internet beginning in 1969.
Analog	Transmission method in which the signal amplitude varies.
Application Service Provider	A company that offers individuals or enterprises access over the Internet to applications and related services that would otherwise have to be located in their own personal or enterprise computers.
Asynchronous	Data transmission one character at a time, with intervals of varying lengths between transmittals; start and stop bits at the beginning and end of each character control the transmission.

Asynchronous Digital Subscriber Line (ADSL)	DSL that has different downstream and upstream speeds. Downstream speeds are usually faster.
Asynchronous Transfer Mode (ATM)	A high-speed, connection-oriented switching technology that can transmit voice, video, and data traffic simultaneously through fixed-length packets called cells.
Attachment Unit Interface (AUI)	A db15 connection on an Ethernet hub that allows the connection of a transceiver for media conversion. (e.g., allows twisted pair hub to connect to fiber or 10base2.
Attentionuation to Croos-Talk Ratio (ACR)	Attenuation to cross-talk ratio The comparison of signal loss to noise interference. The greater the ACR, the better the cable performance will be.
Attenuation	The loss of signal in a cable segment due to resistance, length, poor connections, and other electrical conditions.
Authentication	The verification of the identity of a user or process.
Authorization	The validation of a user, thereby granting access to resources based on user name and password.

B

Bandwidth	The rate at which data signals are transmitted.
Basic Rate Interface (BRI)	An ISDN line that consists of two 64Kbps B (bearer) channels and one 16Kbps D channel.
Bluetooth	Bluetooth is the codename for a proposed standard for wireless communication between devices.
Bootstrap Protocol (BOOTP)	A protocol that lets a network user be automatically configured (receive an IP address) and have an operating system booted (initiated) without user involvement.
Bridge	A device that interconnects local or remote networks forming a single logical network.
Browser	A computer program that allows viewing hypertext documents and "web pages" on the World Wide Web and the Internet.
Bus	A topology where traffic is sent in line. For example, 10Base2.

C

Cable Modem	An interface between computer and cable infrastructure that converts the signal traveling over coax to one that can travel over Ethernet. Commonly used to provide Internet connectivity via the Cable TV provider

Cache	A storage mechanism which is used to store web images and text on local devices (PC’s or network appliances) allowing browsers to access this data quickly and without having to re-access the data from its original source.
Campus Network	A network that covers two or more adjacent buildings on a contiguous grounds.
Capacitance	The ability of an electrical component to hold a charge.
Category 3 (CAT3)	Twisted-pair cable with transmission characteristics specified up to 16 MHz
Category 4 (CAT4)	Twisted-pair cable with transmission characteristics specified up to 20 MHz.
Category 5 (CAT5)	Twisted-pair cable with transmission characteristics specified up to 100 MHz.
Category 5e (CAT5e)	Twisted-pair cable with transmission characteristics specified up to 100 MHz approximately 3db greater signal strength than regular Category 5.
Category 6	Twisted-pair cable with transmission characteristics specified up to 200 MHz. Proposed standard.
Category 7 (CAT7)	Twisted pair cable with transmission characteristics specified up to 600 MHz. Proposed standard.
Cathode Ray Tube (CRT)	Is a specialized vacuum tube in which images are produced when an electron beam strikes a phosphorescent surface.
Cenral Office (CO)	The building where the local telephone company's switching equipment is located.
Certified Service Provider (CSP)	A company that is authorized to sell ANX services.
Channel Service Unit (CSU)	Telecommunications device used for interfacing to a T1 line. Provide test loop point for circuit provider.
Client	A computer on a network that requests services from a server.
Color-Code	A color-coded system for communications cable. The first five pairs are blue, orange, green, brown, and slate. Binders of five pairs each are contrasted by white, red, black, yellow, and violet. For instance, the first pair has a white/blue wire and a blue/white wire the second pair has a white/orange wire and an orange/white wire. The first pair of the second binder has a red/blue wire and a blue/red wire, and so on.
Compact Disk Read Only Memory (CD-ROM)	A storage medium based on the digital music recording specification.

Complementary Code Keying (CCK)	A modulation scheme used with wireless networks (WLANs) that employ the IEEE 802.11b specification. In 1999, CCK was adopted to replace the Barker code in wireless digital networks.
Connecting Block	Also called a terminal block, a punch-down block, a quick-connect block, or a cross-connect block. A plastic block containing metal wiring terminals, which establish connections from one group of wires to another. There are several types of connecting blocks: 66 (split 50), 110, BIX, etc. A connecting block has insulation displacement connections, which means the insulation does not have to be removed from around the wire conductor before it is "punched down" (terminate it).
Cross-Connect	Distribution system used to terminate and connect communication circuits. Patch cords, jumper wire, or fiber optic patch cords are used. The cross-connect is located usually located in an equipment room or wiring closet.
Crosstalk	The "signal bleed" or "noise" of one pair of wires to another though induction. In voice applications this is experienced when hearing a conversation from another line. In data applications it can slow or inhibit signal transfer. Twists in the pairs of wires greatly reduce this effect
Customer Premises Equipment (CPE)	Customer-owned telecommunications equipment such as the CSU/DSU, router, etc.

D

Data Communications Equipment (DCE)	Telecommunications equipment such as a modem, CSU/DSU, etc., that are capable of establishing and maintaining a connection. Converts carrier signal to DTE.
Data Service Unit	A DCE device that converts a high-speed data line to a serial interface (V.35, RS-232, RS-530, etc.) for connection to a router or DTE.
Data Terminal Equipment	Devices such as computers, terminals, and multiplexers, which are the destination end of a remote network. A DTE connects to a DCE such as a DSU or modem.
Dealer Management System (DMS)	A DMS is a software system that manages a dealerships day-to-day business activity
Decible (db)	Unit of measurement that compares an input signal to an output signal. Used to measure attenuation
Dedicated Line	A 24-hours-a-day/7-days-a-week non-switched permanent connection from one point to another.
Demarcation (D-Marc)	The point at which the telephone company terminates service into a company's building

Demilitarized Zone (DMZ)	A DMZ is a buffer network between the Internet and a company's internal network. Computers and services that are to be accessed by the public are put in the DMZ as a security measure to keep public traffic separate from the internal network.
Dialup	The process used by analog modems to connect to a remote location.
Digital Data Service (DDS)	A leased 56/64Kbps data circuit.
Digital Signal Level One (DS1)	Framing specification used for transmitting data signals over a 1.544Mbps T1 line.
Digital Signal Level Zero (DS0)	Framing specification used for transmitting data signals over a single 64Kbps channel of a T1 line.
Digital Subscriber Line	A high-speed data line that uses a single pair of copper telephone wires
Digital Subscriber Line Access Multiplexer	A device that provides DSL connectivity from the central office to the customer.
Digital Versatile Disc (DVD)	A type of optical disk technology similar to the CD-ROM. A DVD holds a minimum of 4.7 GB of data, enough for a full-length movie.
Digital Video Interface	Is a specification created by the Digital Display Working Group (DDWG) to accommodate analog and digital monitors with a single connector.
Direct Sequence Spread Spectrum (DSSS)	Wireless LAN technology that utilizes multiple frequencies in a consistent configuration.
Domain Name Server	System used in the IP networks for translating names of network nodes into addresses.
Dynamic Host Configuration Protocol (DHCP)	A protocol that lets network administrators centrally manage and automate the assignment of IP addresses in a network
Dynamic IP Addressing	Temporary IP address that is sent to a requesting *DHCP* computer from a pool of IP addresses.

E

E-Commerce	Business that is conducted electronically. The most popular form of E-Commerce is Internet based business transactions
EAP Transport Layer Security (EAP-TLS)	This protocol is similar to EAP but uses mutual authentication by client and server both. This method is very secure because it requires certificates to be installed on the server and the client.
Eavesdrop	Secretly viewing data being transmitted on a network.
Electromagnetic Interference	The interference in signal transmission or reception caused by the radiation of electrical and magnetic fields.

Electronics Industry Association (EIA)	An organization that creates and maintains standards for the electronics industry.
Encryption	The translation of data into a secret code which requires a key for the data to be read.
Ethernet	A local area network, which allows computers, printers, servers, workstations, terminals, and other devices to be connected. Ethernet uses twisted-pair or coaxial cable and runs at speeds up to 10Mbps.
Extensible Authentication Protocol (EAP)	An extension of point to point protocol that supports several authentication methods
Extranet	An extension of internal networks that link companies and provide resources for select users and partners.

F

Far-End Crosstalk (FEXT)	Is an electromagnetic interference (EMI), a type of crosstalk, introduced on UTP by close-by wires, usually running in parallel with the FEXT induced wire. "Far End" refers to the inductance of EMI in the end further from the end being measured on the alternate wire in a pair.
Fast Ethernet	Same as *Ethernet* but runs at a speed of 100Mbps.
Fiber Distributed Data Interface (FDDI)	A 100Mbps token passing LAN standard that uses fiber optic cable.
Fiber Optic Cable	A transmission medium that uses glass or plastic fibers, rather than copper wire, to transport data or voice signals at a high bandwidth. Light pulses are used to transmit these signals, which makes them resistant to interference.
File Transfer Protocol (FTP)	Part of the TCP/IP suite of protocols, used for transferring files between network nodes.
Frequency Hopping Spread Spectrum	Wireless LAN technology that rotates through multiple frequencies.

G

Gateway	A routing device. A device that converts data from one protocol stack to another at the application layer.
Gigabit Ethernet	Ethernet that runs at 1,000Mbps.
Gigahertz (GHz)	A unit of frequency measure equaling 1,000 cycles per second.
Graphical User Interface (GUI)	A computer program designed to be user friendly.

H

Home Run	A horizontal cable run that runs directly back to the communications equipment or MDF.
Horizontal Cable	A cable run horizontally between the work area and the MDF/IDF.
HOST	A computer system that is accessed by a user working at a remote location. Typically, the term is used when there are two computer systems connected by modems and telephone lines. The system that contains the data is called the host, while the computer at which the user sits is called the remote terminal.
Hub	A hardware device, which connects many circuits together. A hub is the core of the star in Ethernet and token ring local area networks.
Hypertext Markup Language (HTML)	A set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.
Hypertext Transfer Protocol (HTTP)	The set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
Hypertext Transfer Protocol over Secure Sockert Layer (HTTPS)	A Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

I

IEEE 802.1 Q	This is a standard for VLAN communications.
IEEE 802.11 b	The industry standard for wireless LAN connectivity.
IEEE 802.3	The industry standard for Ethernet LAN connectivity.
Impedance	The opposition to current flow. The AC version of DC resistance.
Industry Standard Architecture (ISA)	16-bit circuit board slot typically found in desktop computers.
Instant Messaging	A service that allows real-time text chatting and or audio-video communications between individuals or groups.
Insulation	Non-conductive material used to protect wires from short-circuiting.
Integrated Services Digital Network (ISDN)	A switched communication service offered by the telephone company to allow data voice and video traffic from end to end
Intermediate Distribution Frame (IDF)	A wiring arrangement that allows connection to station cabling when it is not feasible to run them all the way to the *MDF*. A larger permanent cable usually runs IDF to the MDF

Internet	Large global network of computers linked together by interconnected communications circuits.
Internet Assigned Numbers Authority (IANA)	The organization under the Internet Architecture Board (IAB) of the Internet Society that, under a contract from the U.S. government, has overseen the allocation of Internet Protocol addresses to Internet service providers (ISPs).
Internet Engineering Steering Group	The IESG is responsible for technical management of IETF activities and the Internet standards process.
Internet Engineering Task Force (IETF)	The IETF is the protocol engineering and development arm of the Internet.
Internet Network Information Center	A cooperative activity between the U.S. government and Network Solutions, Inc., was the organization responsible for registering and maintaining the com, net, and org top-level domain names on the World Wide Web.
Internet Packet Exchange	Network protocol used by Novell Netware. Similar to IP.
Internet Protocol (IP)	IP specifies the format of packets, also called datagrams, and the addressing scheme.
Internet Service Provider (ISP)	A company that provides Internet service to consumers and companies.
Intranet	Internal network that provides Internet-style functionality, but it has with no public access.
Intrusion Detection Software (IDS)	Used to provide an indication of a potential or real attack.
Intrusion Prevention Software (IPS)	Which is the next generation of IDS, works more in a real-time environment to identify and STOP attacks.

K

Kilobits per Second (Kbps)	1,000 bits per second.

L

Latency	The amount of delay for a data packet to travel from one node to another and back again.
Layer 2	The Data Link layer of the OSI network standards model. This layer controls dataflow that is taking place on physical devices.
Layer 3	Layer 3 is the Network layer in the OSI network standards model. This layer is responsible for the routing of Internet packets.

Leased Line	A dedicated data line provided by a telephone carrier.
Legacy System	Any old computer system that was set up before your time and now continues to work and need support.
Line Map	The wiring configuration of a jack, block, or patch panel.
Local Area Network (LAN)	A group of computers and devices connected to form network usually limited to inside a single building or campus environment.
Local Exchange Carrier (LEC)	A local telephone service provider.

M

Main Distribution Frame	The spot where the most of the premises wiring is. The MDF is usually located in proximity to the telecommunications equipment.
Media Access Control Address	A hardware address that uniquely identifies each node of a network.
Media Access Controller (MAC)	The Media Access Control (MAC) sub layer is the part of the OSI network model data link layer that determines who is allowed to access the physical media at any one time. It acts as an interface between the Logical Link Control sub layer and the network's physical layer.
Megabits per second (Mbps)	A measure of transmission capacity.
Megahertz (MHz)	See Frequency.
Message Integrity Code	In wireless communications the term Message Integrity Code or MIC is used to refer to a cryptographic checksum used in the handshaking process.
Minimum Point of Entry (MPOE)	Spot at which telephone circuits are normally terminated in order to allow the least amount of work by the LEC inside the building.
Modular Jack	A female receptacle with metal pin conductors used to make an electrical connection between communications circuits.
Modular Plug	A male connector with metal pin conductors used to make an electrical connection between communications circuits.
Modulator-Demodulator (Modem)	A device that converts a digital signal to analog and vice versa, allowing computer data to be transmitted over voice lines.
Multiplexer	A device that combines multiple signals together for transmission over a single channel.
Mux Multiplexer	See Multiplexer.

N

Network Address Translation	The process of converting private addresses to public ones.
Network Interface Card (NIC)	A printed circuit board that allows a computer to communicate with the network.
Network Termination, type 1 (NT1)	A device on and ISDN network that provides the interface between the customer's and the carrier's networks.
Network Traffic	Network Traffic refers to the IP packets that are being transmitted over the network medium. Network traffic can come in other forms in shared mediums such as cable Internet connections where TV signals will also travel over the same medium.
NetworkDrop	The physical extension of the LAN where computer and other network devices can be plugged into the network.

O

OEM	Original Equipment Manufacturer
Operating System (OS)	An operating system (OS) is a software program that manages the hardware and software resources of a computer. The OS performs basic tasks, such as controlling and allocating memory, prioritizing the processing of instructions, controlling input and output devices, facilitating networking, and managing files.

P

Packets	A logical grouping of information containing information used for transmission of the information as well as the data that is being transmitted.
Patch Cord	A cord or cable used to cross-connect patch panels and connecting blocks to communications equipment. Also used to connect the workstation to the wall jack.
Patch Panel	A panel that allows easy connecting and re-connecting between horizontal cabling and communications equipment using modular cords.
Peripheral Component Interconnect	A popular standard for connecting peripheral devices to a processing unit.
PersistentConnection	A connection to the Internet that is always connected.
Personal Digital Assistant (PDA)	A handheld device that provides personal management programs like address book, calendar, and scheduling tools.

Personal Earth Station (PES)	A device that provides access to a satellite network.
Phishing	A form of e-mail fraud where the perpetrator sends out legitimate-looking e-mails that appear to come from well known and trustworthy Web sites in an attempt to gather personal and financial information from the recipient.
Plain Old Telephone Service	A two-wire analog telephone line.
Platform for Internet Content Selection	A specification created by W3C that uses metadata to label webpages to help parents and teachers control what children and students can access on the Internet.
Point-to-Point Protocol (PPP)	Defined in RFC 1661, provides a method for transmitting packets over serial point-to-point links.
Port Address Translation (PAT)	Port Address Translation (PAT) is a feature of a NAT device that translates TCP or UDP connections made to a host and port on an outside network to a host and port on an inside network.
Premises Wiring	The entire wiring system on the user's premises, including that which connects to the network interface. Sometimes referred to as "in-house wiring".
Primary Rate Interface (PRI)	Primary Rate Interface An ISDN line that consists of 23 64Kbps B channels and one 64 Kbps D channel over a T1 transport.
Private Branch Exchange (PBX)	A telephone switchboard that is located on the customer’s premises used to connect to both public and private telephone networks.
Protected EAP (PEAP)	This protocol uses a secure tunneled mode. It supports optional client side certificates in addition to server side ones and the possibility of "single sign-on" with supporting environments.
Protocol	A set of standards governing the communication between network devices.
Proxy	A service or device that permits an administrator to allow or deny applications over the Internet.
PVC	Permanent Virtual Circuit A permanent logical connection between two network devices.

Q

Quality of Service	Performance measurement for a transmission system based on the quality of service and uptime.

R

Remote Monitoring	Specification for monitoring networked devices.
Retail System Provider (DMS)	Third-party supplier of business and operations software to the dealership
Right of Way	Permission to run networking cables across public or private land and infrastructure in order to connect multiple buildings.
RJ11C	Two-conductor modular jack. Typically used for voice applications.
RJ14C	Four-conductor modular jack. Typically used for voice applications.
RJ21X	A 50 pin 66 block that terminates to a 50 pin amphenol connector mounted on the side, typically used by the telephone company as the customer network interface.
RJ25C	Six-conductor modular jack. Typically used for voice applications.
RJ31X	Eight-position modular jack with shorting pins that allows the telephone line to pass through to another device when unplugged. Typically used by burglar-alarm systems.
RJ45	Eight-position modular jack. Typically used for data applications.
Router	A Network device that acts as the traffic cop on a network, directing data packets to the proper destination from LAN to LAN or LAN to WAN.
Routing	Directing of network traffic.
Routing Information Protocol	Protocol used by routers to determine a path to a network by using the route with the least "hops".
Routing Table	A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed.
RS-232	An *EIA* standard for serial connectivity.

S

SC Connector	A type of fiber-optic connector
Scalability	The potential for a network size or features to be increased or decreased in order to meet the changing needs of the dealership.
Secure Sockets Layer (SSL)	A commonly-used protocol for managing the security of a message transmission on the Internet.

Serial	Data transmission where data characters are transmitted sequentially over a single channel.
Server	Device or software that provides services to other devices or "clients".
Service Level Agreement (SLA)	An agreement between customer and service provider guaranteeing a certain quality of service.
Shielded Cable	Cabling that consists of insulated wires in a metal foil or braided strand sheathing with a ground wire encapsulated by a jacket material.
Shielded Twisted Pair (STP)	See Shielded Cable.
Simple Network Management Protocol (SNMP)	A protocol in TCP/IP for managing network devices.
SOCKS	A protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet.
SPAM	Unsolicited e-mail often referred to as junk e-mail.
SPIM	Defined as SPAM over Instant Messaging. Also know as instant SPAM. Typically, SPIM will contain a link to a website. Filtering SPIM will conserve network bandwidth.
ST Connector	A type of fiber optic connector.
STAR	A network topology where nodes on the network are all connected to a central point.
Station Cable	See Horizontal Cable.
Subnet	A subset of nodes partitioned under a larger network.
Switch	A network device similar to a hub with the ability to filter frames based on destination address.
Switched	Method where multiple nodes share the same bandwidth on a network.
Symmetric Digital Subscriber Line (SDSL)	DSL that provides 1.544Mbps download and upload rate over a single pair of twisted wire.
Synchronous	Form of usually high-speed data communication that uses synchronization bytes instead of start or stop bits to tell the receiving device about the coming transmission.

T

T1	A high-speed digital data circuit operating at 1.544Mbps consisting of 24 64Kbps channels.

T568A	A standard eight-position wiring configuration typically used for voice applications.
T568B	A standard eight-position wiring configuration typically used for data applications.
Telecommunications Industry Assocation (TIA)	An organization that develops standards for telecommunication technologies.
Telnet	A terminal emulation protocol that allows remote connections to systems.
Temporal Key Integrity Protocol (TKIP)	The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs.
Terminal	A device that transmits and receives information over a network.
Terminal Server	A processor that connects devices such as printers, terminals, and hosts to a LAN or WAN.
Termination	The connection point at the end of a cable onto a jack or patch panel.
TIA-568-A	A multi-product, multi-vendor, standard for connectivity put forth by the EIA/TIA in 1991 that includes category 3, 4, 5, 5e specifications.
Token Ring	A network topology where nodes are connected to each other in a loop.
Toll Bypass	Leveraging the WAN or VPN to use voice services in order to bypass telephone/long distance toll charges.
Top-level Domain (TLD)	On the Internet, a top-level domain (TLD) identifies the most general part of the domain name in an Internet address.
Topology	The physical layout of the nodes in a network.
Transceiver	A device that provides an interface between an AUI port and standard Ethernet medium.
Transmission Control Protocol / Internet Protocol (TCP/IP)	A set of protocols developed to facilitate data flow between multiple networks and computers.
TSB-67	Technical service bulletin issued by the TIA-568-A entitled "Transmission Performance Specifications for Field Testing of Unshielded Twisted-Pair Cabling Systems." This document specifies cable tester requirements and outlines minimum electrical characteristics of twisted-pair cabling.
TSB-95	Technical service bulletin issued by the TIA-568-A titled "Additional Transmission Performance Specifications for 100 ohm 4-Pair Category 5 Cabling." This document further specifies requirements and characteristics of category five cabling for use with 1000BaseT.

Tunneling	Method of establishing a secure encrypted connection between two network devices.
Twisted Pair	Two insulated copper wires twisted around each other to reduce induction (thus interference) from one wire to the other. These two wires complete an electrical loop. Several sets of twisted pair wires may be enclosed in a single cable.

U

U Interface	The connection on an ISDN BRI device that can plug directly into the network interface without the use of a NT1.
Uniform Resource Locator (URL)	Text name for website location (e.g.,www.yahoo.com).
Uniterruptible Power Supply	A device that stores electricity to supply power to other devices in case of a power failure.
Universal Serial Bus (USB)	A serial bus standard developed to attach personal computers to keyboards, printers, and other peripherals, delivering power to devices on the bus and eliminating separate power cords. The USB standard supports up to 127 devices. USB delivers complete plug-and-play capabilities to electronic devices as well as hot-swap capability. USB 2.0, also referred to as Hi-Speed USB, is an external bus that supports data rates up to 480 Mbps. USB 2.0 is an extension of USB 1.1 specification. USB 2.0 is fully compatible with USB 1.1 and uses the same cables and connectors.
Universal Service Ordering Code (USOC)	A standard for telecommunications industry.
UNIX	A computer operating system developed in 1969 by Bell Laboratories. UNIX is used widely as the OS for many web servers.
Unshielded Twisterd Pair (UTP)	A cord made up of four pair of wires used for many Ethernet networks. Twisted pair currently comes in Categories 1–5.
User Datagram Protocol (UDP)	A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP).

V

V.35	A high-speed serial synchronous interface for communication between a network access device and the network.
Value Added Reseller (VAR)	A company which sells something (e.g. computers) made by another company (an OEM) with extra components added (e.g. specialist software).

Virtual Local Area Network (VLAN)	A group of devices on more than one LAN that are configured so they communicate as if they are on the same wire.
Virtual Private Network	A network over public lines that is secured by encrypting all data that is transmitted from network to network.
Virus	A malicious computer file that negatively impacts the performance of the computer.

W

Wi-Fi	An additional standard to the 802.11b ensuring interoperability between manufacturers.
Wide Area Network	An extension of the LAN to a remote location over high-speed data connection.
Windows Product Activation (WPA)	Is the mandatory product registration system included in Microsoft's Windows XP, Office XP, and recent Office products (such as Word 2002 or Excel 2002) as a means of enforcing compliance with the company's End User License Agreement (EULA).
Wired Equivalent Privacy (WEP)	A security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.
Workstation	Computer on a LAN, typically a personal computer.
World Wide Web	The World Wide Web is a global, read-write information space. Text documents, images, multimedia and many other items of information, referred to as resources, are identified by short, unique, global identifiers called Uniform Resource Identifiers (URIs) so that each can be found, accessed and cross-referenced in the simplest possible way.

X

xDigital Subscriber Line (XDSL)	Refers to different variations of DSL, such as ADSL, HDSL, and RADSL.