Multi-Extranets: Architecture and Application Domains

Algirdas Pakstas[1]
University of Sunderland, SEAT, Sunderland SR1 3SD, England
Institute of Mathematics and Informatics, LT-2600 Vilnius, Lithuania
E-mail: a.pakstas@ieee.org

Abstract

This paper is devoted to examining of the new emerging area of the Internet use, namely, "extranets". Definitions and examples are given. Notion of multi-extranet is introduced. Open application standards are discussed. Role of network management and security issues are outlined. Existing experience of running intranets is discussed and criteria for choosing planning strategy are suggested. Cost issues are discussed.

I. Introduction: The Third Wave is Coming

Internet has been flourishing very fast indeed and the World Wide Web is growing at an exponential rate. The possibility of the "address crisis" was removed for the foreseeable future by the development of version 6 of the Internet Protocol (IPv6) to replace version 4. However, even in the fast-paced world of the Internet, it is difficult to accept that such a fundamental concept of *intranet*, the so called *second wave*, was introduced just some year ago. During 1996, intranets have been embraced by corporate users of information services and made substantial inroads in strategic vision documents and procurement practices.

The new era of the *extranet*, or the *third wave* of the universal Internet concept has just begun. As a powerful enabler of worldwide electronic commerce, the extranet is poised to trigger a revolution in the structure and operations of commercial enterprises and government organizations.

It is normally said that an *extranet, or extended Internet, is a private business network of several cooperating organizations located outside the corporate firewall.* An extranet service relies on the existing Internet interactive infrastructure, namely servers, E-mail clients and Web browsers. In comparison with the creation and maintenance of a proprietary network this feature makes extranet very economical. Business partners, suppliers and customers who share common interests may form a tight business relationship and a strong communication bond. Web-systems has developed their content and marketing potential and in this sense the term "third wave" also refers to the maturity process in the development of Web technology.

This paper presents some results of the studies on the development of the extranet for the high-technology science park. As an example is used *Sorlandets Teknologisenter (STS)* in Grimstad, Norway with which author is most familiar. The rest of paper is organized as following. Definitions of terms is presented in Section II. Applicable standards are discussed in Section III. A role of Network Management is outlined in Section IV. Section V is devoted to security issues. Section VI discusses experience and recommendations for running of intranets. Cost-relevant issues are presented in Section VII.

[1] This project was partially funded by Agder College, Grimstad, Norway

II. Extranets: Definitions and Examples

According to [1] "Unlike the Internet, an extranet is not wide open. Unlike an intranet, it is not restricted to internal use. An extranet is a state of mind, not a technology." An extranet is a collaborative network that uses Internet technology to link businesses with their suppliers, customers, or other businesses that share common goals e.g. to allow customers and/or mobile workers access to the company's data. The term has been used by Jim Barksdale and Mark Andreessen of Netscape Communications to describe software that facilitates intercompany relationships. An extranet can be viewed as part of a company's intranet that is made accessible to other companies or that is a collaboration with other companies. The shared information might be accessible only to the collaborating parties or, in some cases, might be public.

A. Examples of Extranet Applications

Examples of extranet applications might include:

- Shared product catalogs accessible only to wholesalers or those "in the trade".
- Private newsgroups that cooperating companies use to share valuable experiences and ideas.
- Groupware in which several companies collaborate in developing a new application program they can all use.
- Project management and control for companies that are part of a common work project.
- Training programs or other educational material that companies could develop and share.

Thus, a term "extranet" refers to an intranet that is partially accessible to authorized outsiders. Whereas an intranet resides behind a *firewall* and is accessible only to people who are members of the same company or organization, an extranet provides *various levels of accessibility to outsiders*. You can access an extranet only if:

- you have a valid *username* and *password*, and
- your identity determines *which parts of the extranet you can view*.

Finally, Table 1 summarizes discussed features of Internet, intranet and extranet.

Table 1. Summary of the Internet, Intranet and Extranet features

	Internet	Intranet	Extranet
Access	Public	Private	Semi-private
Users	Everyone	Members of the specific firm	Group of closely related firms
Information	Fragmented	Proprietary	Shared in closely trusted held cicles

B. Extranets and Intergroupware

Groupware is a class of software that provides functions to aid workgroups. These include *Communications*, *Collaboration*, and *Coordination*. Emphasis is on computer-based augmentation of human communications and information sharing, and support of generic workgroup tasks like scheduling and routing of message-based workflow tasks. *Intergroupware* is just groupware applied with the flexibility to support multiple interacting groups, which may be open or closed, and which may share communications selectively, as appropriate (as in an extranet). It can be noted that intranets and extranets are generally not very meaningful as *categories of networks*. As an alternative, we should think of them as *classes of applications*: intranet, extranet, and public Internet applications will all run on the same network infrastructure, but their content (program and data) resources will be administered for different levels of accessibility and security.

The diagram in Fig.1 is intended to clarify whole the picture. It shows the distinct forms of electronic media, the kinds of interactions they support, and how they are converging. In the enterprise communications the inter- and intra- organizational media-based communications activities are forming two separate parallel *planes*. The dimensions of each plane are the degree of *structure* and the degree of *mutuality* in the communications activities.

- *Structure* lies between informal (ad-hoc) and formally structured, defined, and managed or edited processes.
- *Mutuality* ranges from unidirectional or sequential back-and-forth message passing, to true joint work or *collaborative transactions* in a shared space of information.

The resulting *four regions* characterize *four different kinds of interaction*, which place distinct demands on their media vehicles or tools. Separate tools have developed in each region as pointsolutions, but the need to apply them widely and in concert is causing them to converge. Groupware has been understood in terms of "the three C's," which correspond to three of mentioned four quadrants. These are:

- *Communications or messaging* (notably email),
- *Collaboration or conferencing* (notably forums or " bulletin board" systems which organize messages into topical " threads" of group discussion, maintained in a shared database), and
- *Coordination or workflow and transactions* (applying pre-defined rules to automatically process and route messages).

The success of Lotus Notes stems from its recognition that, while these have distinct characteristics, they can only be served effectively by a unified platform that allows them to interact seamlessly.

C. Multi-extranet As A New Artifact

According to the current ideas about functioning of the STS it is expected that three types of organizations will use its facilities:

1. "Normal" firms which will have their own intranets and access to the Internet either on their own or via STS facilities.
2. "Small" firms which will obtain access to the Internet via STS facilities and with the only intranet which will be actually extranet.
3. "Large" firms such as Telenor, Ericsson, etc. which will, perhaps, not bother to be connected to the STS facilities at all.

This situation is depicted in Fig.2. Here F1 and F2 are examples of "normal" firms, F3 is example of small firm and, finally, F4 is example of large firm.

Firewalls between intranets In1, In2 and In4, and Internet are in this case property and responsibility of their owners. Extranets Ex1, Ex2 and Ex3, in contrast, are responsibility of STS. In order to regulate the rights of access to these extranets for different categories of users it is presumed that *Access Daemon* should be provided for each extranet. It is unclear on the current stage of study if some *Common Access Daemon* is feasible (i.e. such daemon which will function as "Yellow Page" service or common access interface for all the firms covered by STS services).

We suggest a new term such as M*ulti-extranet* (or *multiXnet*) for this class of systems and we can expect that such studies will arise in similar environments of Hi-Tech Science Parks, Technological Incubators, etc., i.e. where many (often start-up) firms will share common infrastructures and in the same time will be interested in developing of common profile. In this case we will define that STS's multiXnet STSmXn, is superposition of involved extranets, i.e. STSmXn = Ex1 + Ex2 + Ex3 or in general case for the Organization O: 0mXn = SUM(Xi).

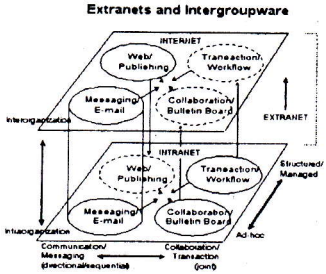

Figure1 - Relations between extranets and intergroupware

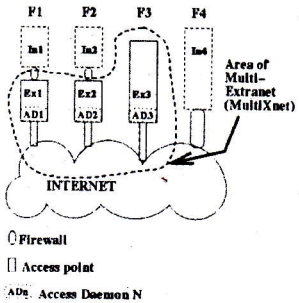

Figure 2 - Architecture of MultiXnet. Here: F1..F4 - firms; In1, In2 - intranets; Ex1, Ex2 and Ex3 – extranets.

III. Open Application Standards

A. Available Standards

Broad use of the Internet technology is now supported by the existence of *the open application standards* that offer a range of features and functionality across all client and server platforms:

- Platform-independent *content creation, publishing and information sharing*: HTML and HTTP.
- Platform-independent *sofware development* as well as *creation and deployment of distributed objects*: Java, JavaScript, Common Object Request Broker Architecture (CORBA).
- Platform-independent *messaging and collaboration* (E-mail, discussion, and conferencing capabilities): Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Multipurpose Internet Mail Extensions (MIME), Secure MIME (S/MIME), Network News Transport Protocol (NNTP), Real Time Protocol (RTP).
- *Directory* and *security services, netwvork management capabilities*: Lightweight Directory Access Protocol (LDAP), X.509, Simple Network Management Protocol (SNMP).

Netscape Communications offers a suite of applications (called "AppFoundry") that it says are designed for possible extranet use. Thus, here the term "extranet" perhaps puts a name on a phenomenon that already existed informally in various intercompany groupware. *Lotus Notes* is another product or set of products that would seem to support extranets.

B. Netscape's Choice

Netscape's partners have agreed on a collection of standards and "best practices" for use in extranet deployment and creation of *Crossware*. For enterprises, this offers two significant benefits:

- An assurance of interoperability among products from multiple vendors.
- A virtual roadmap for efficient implementation of an extranet.

Netscape's partners have committed to support the following Internet standards: LDAP, X.509 v3, S/MIME, vCards, JavaSoft, EDI INT (see Appendix). Together, these standards create a comprehensive infrastructure that enables Crossware applications to interoperate across the Internet and the intranets of business partners, suppliers, and customers.

They also serve to provide a secure environment that supports much more than simple exchange of HTML pages between enterprises. In fact, the standards agreed upon by Netscape's partners represent by far the most secure, as well as the best supported, open standards technology.

To summarize:

- Open standards provide the most flexible, efficient, and effective foundation for enterprise networking.
- Enterprise intranets have exhibited clear benefits and are becoming ubiquitous.
- Netscape believes that extranet technology represents the optimal future for enterprise networking.
- Claimed goal of Netscape and its partners is *"to assist enterprises in the deployment of secure, effective extranets".*

IV. Role of Network Management

Network Management refers to the broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including:

- *Security*: Ensuring that the network is protected from unauthorized users.
- *Performance*: Eliminating bottlenecks in the network.
- *Reliability*: Making sure the network is available to users and responding to hardware and software malfunctions.

Network management systems have been in operation many years especially in their own proprietary worlds such as Netview, AT&T Accumaster and Digital Equipment Corporation's DMA. With the implementation of SNMP, local area and wide area network components could be monitored and "managed" . With the vast amount of raw data available, most IT Managers have no idea what they really want because, in part, they don't know what's available. Additionally, how does the data get into a format that actually means something? Other communications systems are considered non-manageable because they are only accessible by an RS-232 port and not by Netview or SNMP. Others tend to believe that Network Management means nothing but the monitoring and management of network architectural hardware such as routers, bridges and concentrators - nothing above the network layer of the OSI model is considered manageable.

What's alarming is that most Senior Network Engineers tend to be resigned to spend thousands of dollars on hardware and software before the real requirements are gathered and defined. Consequently, IT departments either spend very little on network management or they "go for broke" with the huge hardware platforms and expensive artificial intelligence engines driving network management for the company.

A. Network Management Technologies

The task of a management technology is to support the management of resources in a distributed environment - to enable a *manager system* to gather information about the *resources* it manages and to exercise control over them. These resources are typically in or under the direct control of some other computer system or system component, termed the *managed system* or *agent*, with which the manager system communicates. (In a CORBA environment, these system elements are objects.)

Specifications of management technologies typically cover the *communications protocols* between manager and managed systems, and the *management information* that defines requests for management operations, the results of the operations and unsolicited reports such as

alarms. Existing Network and System Management solutions are based on different management technologies. The most common technologies are:

- OSI Management,
- Internet Management
- CORBA/OMG.

In large enterprises (e.g. Telecommunication Service Providers), system and network managers are more and more having to deal with heterogeneous communication and information processing environments where more than one management technology is in use. Hence there is an urgent need for strategies for *coexistence* and *convergence* between the technologies.

B. OSI Management

The OSI Management technology enables manager systems to monitor and control resources by sending operation requests to managed systems, and it enables managed systems to send event reports when important things happen to the resources. It has mechanisms for increased efficiency that make it possible to send a number of operation requests in a single communication, to filter out less significant event reports under management control, to log events locally, and to summarize information.

It uses the OSI CMIP protocol to carry the management information over a data communication network. CMIP may be supported by a full 7-layer OSI stack or by other means. The OSI management information model uses an object-oriented approach to represent how real-world systems and resources can be managed, in the form of *managed objects*, which are defined using the ISO/IEC & ITUT Guidelines for the Definition of Managed Objects (GDMO), together with Abstract Syntax Notation One (ASN.1).

OSI management also includes a number of specifications aimed at increasing consistency in the way different resources are managed, such as a common format for alarms and a common state model. These are termed *systems management functions*.

C. Internet Management

The IETF has specified a number of RFCs that define how network management is to work in the TCP/IP environment. Its basic protocol is SNMP (Simple Network Management Protocol), with a second version, SNMP2, now under development as a draft Internet standard.

The Internet Management model adopts a manager/agent approach where the agents maintain information about resources and managers request information from the agents. The Internet Structure of Management Information (SMI) standard specifies a methodology for defining the management information contained in the Management Information Base (MIB). SMI uses a subset of ASN.1 data types. The MIB defines the elements of management information as variables and tables of variables.

D. CORBA/OMG

The Object Management Group (OMO) has developed an object-based environment for the development of distributed systems, which includes CORBA (the Common Object Request Broker) and IDL (an Interface Definition Language) for specifying the interface to objects. The initial release of CORBA does not specify a particular protocol for communication between objects that are in different systems but assumes use of a standardized protocol (although later versions of CORBA will specify particular protocols). The CORBA IDL can be used to specify objects related to management. CORBA also includes management-related services such as Naming and Event services.

E. Management Coexistence and Convergence

Efforts are under way to show how the diverse technologies that have been developed can coexist, and perhaps converge to provide a single management environment. One important activity has been the specification (developed by the NMF) of a simple mapping between managed objects defined using GDMO and those defined using Internet SMI. This approach allows gateways to be built between networks using OSI and Internet Management technologies.

A further key activity is the development by the Joint Inter-Domain Management (JIDM) task force, with membership from the NMF and X/Open, of a document (Inter-Domain Management Specifications, Specification Translation - currently an X/Open preliminary specification) that provides translation algorithms for converting (in both directions) between the IDL used for CORBA objects and GDMO for OSI managed objects, and between SNMP MIBs and IDL (only in one direction). Future work will specify the dynamic conversion requirements (e.g. how to convert CMIP PDUs to operations on CORBA objects).

EWOS is an open European organization working to provide high quality contributions to the worldwide efforts to build an effective Global Information Infrastructure, whilst ensuring proactive support of solutions meeting specific European needs, in areas such as Electronic Commerce.

V. Network Security Issues

Network administrators have increasing concerns about the security of their networks when they expose their organization's private data and networking infrastructure to Internet crackers. The term *security* in general refers to techniques for ensuring that data stored in a computer cannot be read or compromised. Most security measures involve *data encryption* and *passwords*. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Security has become one of the primary concerns when an organization connects its private network to the Internet. Regardless of the business, an increasing number of users on private networks are demanding access to Internet services such as the World Wide Web (WWW), Internet mail, Telnet, and File Transfer Protocol (FTP). In addition, corporations want to offer WWW home pages and FTP servers for public access on the Internet.

Thus, we would like to conclude with the following citation: *"A corporation needs to protect its competitive information assets while at the same time optimizing its information exchange. Security should not be a reason for avoiding cyberspace, but any corporation that remains amateurish about security is asking for trouble [2]".*

Solving security problems normally involves the following actions:

1. Risk assessment procedure should answer the following typical questions: What are organization 's most precious intellectual and network assets? What do you need to protect, and what protocols are involved? Next, where do your assets reside? What's the risk if they are subjected to unauthorized access? How much damage could be done - can it be quantified in currency units (dollars)?

2. Security policy. To provide the required level of protection, an organization needs a security policy to prevent unauthorized users from accessing resources on the private network and to protect against the unauthorized export of private information. Even if an organization is not connected to the Internet, it may still want to establish an internal security policy to manage user access to portions of the network and protect sensitive or secret information. According to the FBI, 80 percent of break-ins are internal. Rules and policy should be set by business managers, the Chief Information Officer and a security specialist - someone who understands policy writing and the impact of security decisions.

A firewall is an implementation of *access rules*, which are an articulation of your security policy. It is important to make sure that firewall vendor supports all the necessary protocols. If LANs are segmented along departmental lines, firewalls can be set up at the departmental level. However, one LAN often accommodates multiple departments. In this case, creation of virtval private network (VPN) for each person is highly advisable.

Following are recognised as a **basic steps for developing a security policy**:

1. Assessment of the types of risks to the data will help to identify weak spots. After correction, the regular assessments will help to determine the ongoing security of the environment.

2. Identification the vulnerabilities in the system and possible responses, including operating system vulnerabilities, vulnerabilities via clients and modems, internal vulnerabilities, packet sniffing vulnerabilities and means to test these vulnerabilities. Possible responses include encrypting data and authenticating users via passwords and biometrically.

3. Analysis the needs of user communities. Grouping data in categories and determining access needs. Access rights make the most sense on a project basis. Determining the time of day, day of week and duration of access per individual are the most typical procedures. Determination and assignment of the security levels can include the following, five levels:

- level one for top-secret data such as prereleased quarterly financials or a pharmaceutical firm's product formula database
- level two for highly sensitive data such as the inventory positions at a retailer
- level three for data covered by non-disclosure agreements such as six month product plans
- level four for key internal documents such as letter from the CEO to the staff
- level five for public domain information

It is recommended to put firewalls at the personal desktop, workgroup, team, project, application, division, and enterprise level.

4. Writing the policy.

5. Development a procedure for revisiting the policy as changes are made.

6. Writing an implementation plan.

7. Implementation of the policy.

3. Authentication, Authorization, Encryption. Involving of encryption requires introduction of the key management/updating procedure. Encryption can be implemented:

- *At the application*: Examples of this are Pretty Good Privacy (POP) and Secure Multipurpose Internet Mail Extensions (S/MIME), which provide encryption for e-mail.
- *At the client or host network layer*: The advantage of this approach is that it will provide extra protection for the hosts that will be in place even if there is no firewall or if it is compromised. The other advantage is that it allows to distribute the burden of processing the encryption among the individual hosts involved.

  This can be done on the client with products like Netlock (see www.netlock.com), which provide encryption on multiple operating system platforms at the IP level. System can be set up so that it will only accept encrypted communications with certain hosts. There are similar approaches from Netmanage, and FTP Software.
- *At the firewall network layer*: The advantage to this approach is that there is centralized control of encryption which can be set up based on IP address or port filter. It can cause a processing burden on the firewall, especially if a lot of streams that have to be encrypted or decrypted. Many firewalls come with a feature called virtual private network (VPN). VPNs allows encryption to take place as data leaves the firewall. It has to be decrypted at a firewall on the other end before it is sent to the receiving host.
- *At the link level*: The hardware in this case is solely dedicated to the encryption process, thus off-loading the burden from a firewall or router. The other advantage of this method is that the whole stream is encrypted, without even a clue as to the IP

addresses of the devices communicating. This can only be used on a point to point link as the IP header would not be intact which would be necessary for routing.

Products like those manufactured by Cylink encrypt data after it leaves the firewall or router connected to a WAN link.

Finally, Table 2 provides summary of the weak points in the system security, identifies and shows how these problems can be addressed and suggest technical solutions for them.

- Table 2. Weak points and security hazards

Weak Point/Hazard	Technical Solution
Operating system/ applications on servers	Research vulnerabilities; Monitor CERT advisories; Work with vendors; Apply appropriate patches or remove services/applications; Limit access to services on host and firewall; Limit complexity
Viruses	Include rules for importing files on disks and from the Internet in security policy; Use virus scanning on client, servers and at Internet firewall
Modems	Restrict use; Provide secured alternatives when possible (such as a dial-out only modem pool)
Clients	Unix: Same as server issues above; Windows: for Workgroups, Win95, NT: Filter TCP/UDP ports 137,138,139 at firewall; Be careful with shared services, use Microsoft's Service Pack for Win95 to fix bugs
Network snooping	Use encription; Isolate networks with switch or router
Network attacks	Internet firewall; Internal firewall or router; Simple router filters that don't have an impact on performance
Network spoofing	Filter out at router or firewall
Additional reading	NCSA's Publication Catalog: http://www.ncsa.com/catalog/catgenerity.html Netware security: http://alcpress.com/, http://www.davidson.net/cgi-bin/vlink/1562055453 Windows NT security: http://www.trustedsystems.com/NTBook.htm Unix security: http://www.davidson.net/cgi-bin/vlink/0130153893 Database security: http://www.elet.polimi.it/section/compeng/db/security/book.html Know your enimy: http://www.26000.com, http://www.hackerscatalog.com/books.html

VI. Experience and Recommendations for Running of Intranets

A. Intranet Applications and Their Obstacles

Delphi Consulting Group, which is a company advising large and small corporations on the directions of their document management strategies, has reported results of their survey on installed intranet applications. In Delphi's recent survey [3] of over 600 users/evaluators of electronic document management systems, 65% had intranets in place and only a mere 6% had no plans to install an intranet over the next two years. Currently, less than half of all organizations surveyed had more than 50% of their desktops connected to an intranet. But, these organizations projected that by the year 2000 (three years away), over 82% of all organizations will have 75% or more of their users connected to an intranet. The most common usage of the intranet among those organizations surveyed by Delphi was as a means to share internal information (see Fig.3). However, amongst all of the widespread acceptance and positive outlooks expressed by the survey respondents, caution regarding frustrations and hurdles to intranet acceptance were also expressed (see Fig.4).

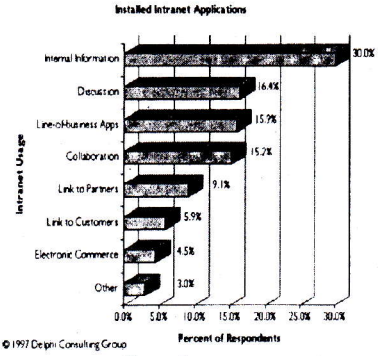

Figure 3.

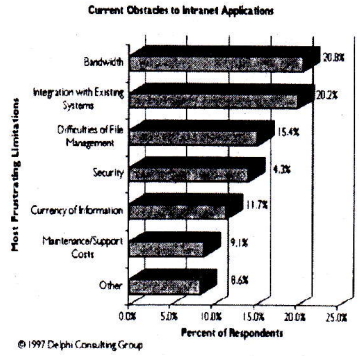

Figure 4.

As might be expected, the eternal problem of bandwidth capacity topped the user's list of frustrations. But this problem can be easily dealt with, and will surely be met by various "solutions" from hardware and telecommunications vendors in a relatively short time frame. A more significant set of problems dealing with the practical aspects of developing meaningful mission critical applications over the intranet fall just beneath the bandwidth dilemma. These range from the inability to integrate Web-based applications and legacy systems, to the vulnerability of intranet information (e.g. security and currency).

B. Criteria for Choosing of Planning Strategy

Delphi's survey presented above covers much wider group of companies than we ever can expect at the STS - 600 surveyed by Delphi vs. cat 100 expected in STS in the coming 2 years. Thus, practice observed by the survey can be accepted by us as representative set for future considerations.

Futhermore, based on the Delphi's survey we suggest that it might be reasonable to focus on the "top 5" approach, i.e. select 5 upper parameters shown in the diagrams as a guidelines for our choices. In this case a diagram "Installed Intranet Applications" helps us to identify the most important usages of intranets/extranet: *Internal Information Exchange, Discussions, Line- of-business Applications, Collaborations* and *Link to Partners.*

Surprising enough is the fact that other two, such as *Link to Customers* and *Electronic Commerce* (which according to it common definition sounds vital for any extranet) doesn't fall into category of most important intranet usages! Not yet...

Considering observed limitations of intranets we note that here "top 5" group identifies the following problems: *Bandwidth, Integration with Existing Systems, Difficulties of File Management, Security* and *Currency of Information.*

Bandwidth problem can be solved relatively easily. *Integration with Existing Systems and Difficulties of File Management* are problems of the same nature caused by bringing "unnetworked" organization to the intranet. It can be completely solved by choosing appropriate application standards and tools. *Security* problem while will be essentially resolved by appropriate protocols and tools will still require regular activity of network managers who are responsible for it. The last problem, *Currency of Information,* is rather organizational which, perhaps will stay unsolved forever if no appropriate information/ document flow management policies and tools are applied by the organization.

VII. Cost Issues: Facts and Models

This Section will examine cost-relevant issues important for the infrastructure and operation of extranets and multixnets such as STS.

A. Cost of Running Web Site

Evolutionary scale of Web sites suggested by the Positive Support Review Inc. of Santa Monica, CA [4] includes the following:

1. *Promotional*: A site focused on a particular product, service or company. Cost: $300,000$400,000 per year (17-20% on hardware and software, 5-10% on marketing, and the balance on content and servicing).
2. *Knowledge-based*: A site that publishes information that is updated constantly. Cost: $1 to $1.5 million annually (20-22% on hardware and software, 20-25% on marketing, and 55-60% on content and servicing).
3. *Transaction-based*: A site that lets surfers shop, receive customer services or process orders. Cost: $3 million per year (20-24% on hardware and software, 30-35% on marketing, and 45-50% on content and servicing).

A similar classification by Zona Research Inc. of Redwood City, CA (cited in [5]), divides Web sites into:

1. *Static presence ("Screaming and Yelling ")*. According to Zona Research, page cost for such sites is less than $5,000. At present, the absolute majority of Web sites belong to this category.
2. *Interactive ("Business Processes and Data Support")*, with page costs ranging from $5,000 to $30,000. Perhaps 15 to 20% of all current Web sites are in this category.
3. *Strategic ("Large Scale Commerce")*, with dynamic pages that cost more than $30,000 each to produce and maintain. According to the [6], fewer than 0.5% of all Web sites are in this category.

In its latest market research reports (see http://www.zonaresearch. com/) Zona projects multibillion dollars intranet/extranet market expansions till the end of the century.

B. ISDN Cost Model

ISDN should be mentioned as an important technology for building extranet infrastructure because of its ability to support flexible access by the mobile workers. ISDN cost model should consider the following:

- Service fees from local telco for each location (installation + monthly + per minute)
- Long distance charges, if applicable
- Cost of equipment (NT1 + TA, NT1 + bridges, NT1 + routers, etc.)
- Cost of Internet Service Provider (ISP) services, if applicable

Determine your maximum number of connected minutes per month to create a budget, for example, $25 a month + 2 cents per minute per channel. Therefore, you pay $2.40 per hour for two B connections. If you want to be connected three hours per day, 20 days per month, you will need $144 + $25 = $169 for a month of service, just for the local telecom portion of your ISDN connection. Long distance fees and ISP charges would naturally needed to be factored into this as well.

C. Mobile Connection Cost Model

Wireless communications is another option for mobile workers which can be highly cost effective, but its costs generally are higher than wireline communications. With packet data, the modem occupies the radio channel only for the time it takes to transmit that packet. In the

ordinary data networks users are usually billed for the amount of data they send. In contrast, when you use your PC Card modem to communicate over a cellular connection, you are making a circuit connection and *paying for the duration* of the call just as when you make a voice call. The per-minute charges are usually the same.

Wireless modems are complex electronic devices, containing interface logic and circuitry, sophisticated radios, considerable central processing power and digital signal processing. As such, they cost more than landline modems. Most wireless WAN modems cost $500 or more.

D. The Cost of Downtime

Electronic commerce is difficult in case of unreliable infrastructure. In this Section we will use an example from [7] to examine the cost of downtime for some consumer-oriented business, such as an airline's or hotel's reservation center. The customers have a choice. If they cannot reach the reservation center, they will call a competitor and place their order there. Lost business is really gone for good.

Our customer service center has a staff of 500 people, each of which carries a burdened cost of $25 an hour. They make an average of 60 transactions per hour and average of three high-priced sales per hour. Hours of operation are 24 hours a day, seven days a week, 365 days a year.

Table 3. Cost of outages

Downtime percentage	0.9990
Number of hours/year	8.76
Number of employees	500
Average burdened cost	825
Idle sale	$109,500
Impact to production	$131,400
Opportunity lost	$262,500
Total downtime impact	$503,700

Table 4. Impact to production

Profit per transaction	0.5
Transactions per hour per employee	60
Missed transactions per hour	30,000
Total missed transactions	262,800
Impact of missed transactions	$131,400

Table 5. Opportunity lost

Profit per sale	20
Sales per hour per employee	3
Missed sales per hour	1,500
Total missed sales	13,140
Impact of missed sales	$262,600

In actuality, line managers of the site should calculate the costs of downtime, not the IT staff. This information often is not forthcoming, however. So, this example can be presented to give a general sense of the impact that downtime has on the bottom line. The goal is to open some eyes and generate some debate. We can use this example as a guideline for how to estimate the cost of outages in our environment.

As we can see (Tables 3-5), the cost of outages in the hypothetical network with an availability rate of 99.9% is about half a million dollars a year. Let say, we have already bought the hardware and software necessary to do the job. *We can consider this estimate a guideline on the additional budget to spend on providing redundancy.* This is separate and apart from the funds required to provide a base level of network functionality. Thus, it is really not worth rushing headlong into designing a fault-tolerant network unless all parties agree on all the implications that downtime has to the operation. This is the time to seek an executive sponsor to champion the process.

VIII. Conclusions

Extranet is conceptualized as the key technology enabler for the development of the third wave largescale electronic commerce sites. While technical and cost advantages are of very importance, the real significance of Extranet is that it is the first *nonproprietary* technical tool

that can support rapid evolution of *electronic commerce*. It is already clear that the Internet inpacted retail sales, the use of credit cards and various digital cash and payment settlement schemes. However, the experts predict that the real revolution over the next three to five years will be in systems for global procurement of goods and services at the wholesale level and that a role of Extranets is crucial for this. It is also expected that on a more fundamental level the extranets will stimulate the business evolution of conventional corporations into *the knowledge factories*.

Before planning MultiXnet development phases for the STS we should admit that STS is already behind of the most active participants of the intranet/extranet implementation process. However, the rate of deployment of extranets is currently minimal and this fact gives a chance to liquidate the gap reasonable fast. Given the relative immaturity of the intranet itself, it is reasonable to project that great strides will come in this area within the next two years.

Thus, it seems naturally that we allocate 12 months for implementing of **Phase I** and another 12 months for **Phase II**. It is reasonable for **Phase I** to focus on the applications and standards which will helps to solve mentioned "top 5" problems, i.e. on IT infrastructure of the STS, its mobile workers and partners inside the park, common Web-server, normally working intranets in all the partner companies and common E-mail server.

Phase II is devoted to future development of extranet. Developing of links with the customers as well as electronic commerce facilities should not be forgotten but its "flourishing" can be left for the Phase II. After 2 years of fulfilling of such a plan we hopefully will liquidate a gap and will find us on the same development stage together with other intranetactive communities and countries.

IX. References

1. Richard H. Baker, "Extranets: The Complete Sourcebook" .
2. James Martin, "Cybercorp, the new business revolution" .
3. Carl Frappaolo, "Intranets: The Way to a Wider Tomorrow". Delphi.
4. Victor Junalaitis, "The true cost of the Web". PC Week, November 18, 1996, p.85.
5. Esther Shein, "Natural Selection". PC Week, October 14, 1996, p.E2.
6. Netcraft and O'Reilly and Associates, "State of Web Commerce" (http://ssl.netcraft.com/), December 1996.
7. Network Design: Fault Management. (http://techweb.cmp.com/nc/netdesign/faultmgmt.html)

APPENDIX. Internet Standards Supported by Netscape's Partners

A. LDAP

LDAP intelligent directory services store and deliver contact information, registration data, certificates, configuration data, and server state information. These services provide support for single-user logon applications and strong authentication capabilities throughout the extranet. Key benefits:

- Users can search for contact information across enterprises, partners, and customers using the same interface and protocols as internal corporate directories.
- A standard format for storage and exchange of X.509 digital certificates allows single-user logon applications and secure exchange of documents and information via S/MIME.

- Replication over open LDAP protocol allows secure distribution of directory data between enterprises.
- Enables extranet applications that rely on fast and flexible queries of structure information.

B. X. 509 v3

X.509 v3 digital certificates provide a secure container of validated and digitally signed information. They offer strong authentication between parties, content, or devices on a network including secure servers, firewalls, email, and payment systems. They are a foundation for the security in S/MIME, object signing, and Electronic Document Interchange over the Internet (EDI INT). Digital certificates can be limited to operate within an intranet or they can operate between enterprises with public certificates co-issued by the company and a certification authority such as VeriSign. Certificates surpass passwords in providing strong security by: authenticating identity, verifying message and content integrity, ensuring privacy, authorizing access, authorizing transactions, and supporting non-repudiation. Key benefits:

- Digital certificates eliminate cumbersome login and password dialog boxes when connecting to secure resources.
- Each party can be confident of the other's identity.
- Digital certificates ensure that only the intended recipient can read messages sent.
- Sophisticated access privileges and permissions can be built in, creating precise levels of authority for Internet transactions.

C. S/MIME

S/MIME message transmission uses certificatebased authentication and encryption to transmit messages between users and applications. S/MIME enables the exchange of confidential information without concerns about inappropriate access.

D. vCards

vCards provide a structured format for exchanging personal contact information with other users and applications, eliminating the need to retype personal information repeatedly.

E. JavaSoft

Signed objects allow trusted distribution and execution of software applications and applets as part of an extranet. With signed objects, tasks can be automated and access to applications and services within the extended network granted based on capability. A digital certificate is used with a signed object to authenticate the identity of the publisher and grant appropriate access rights to the object.

F. EDI INT

EDI INT provides a set of recommendations and guidelines that combine existing EDI standards for transmission of transaction data with the Internet protocol suite. By using S/MIME and digital signatures, EDI transactions between enterprises can be exchanged in a secure and standard fashion.