CEDPA K-12 TECHNOLOGISTS
http://www.cedpa-k12.org

DataBus

"Supporting California's Educational Technology Community"

Vol. 41 • No. 2 February-March, 2001

Education: The Digital Future

Conference: Theme Addresses Technology Revolution in the Education Environment.

Warren Williams, Grossmont Union High School District

Announcing a digital future might seem strange to those who have been managing digital environments, some for more than twenty years. The change from analog to digital was part of a revolution that preceded the Internet. This revolutionary change occurred in IT departments whose responsibility was to convert language and business rules into bits and bytes. It happened in research institutions that took the language of programmers and created digital hardware that extended human capability. So why is CEDPA, an organization dedicated to bringing the latest information to educational technologists, putting an emphasis on what appears to be an idea that is not new?

The reason can be seen in the democratization of the digital world. Digital information is no longer relegated to the purview of people who have been trained in its developmental intricacies. Students and teachers are daily creating digital movies and animated stories. They don't think about the medium of transport. Things like a seven layer OSI model have no consequence for them. They don't care if their email is LDAP compliant or if their Virtual Enterprise is dependent upon a sophisticated support mechanism. Their wireless connection to a network is an expectation and that excessive collisions can cause a degradation in the speed of their ability to transfer information is an annoyance not an understanding. The educational dynamic – teaching and learning – keeps IT managers engaged in an environment of perpetual change, trying to match limited resources with an insatiable demand.

Legislators are complicit partners in this process. Recognizing that investment in technology can offer dramatic capacity to a system that needs assistance in producing better results. They offer impressive incentives to schools to deploy digital technologies that increase student performance. California has created the Digital California Project (DCP) that at first blush appears to be the development of a high capacity broadband network for K-12. But that is not the real intent of the DCP. Its creators understand that a radical evolution is occurring in education – a digital revolution. Education is about to become virtual and the first state to provide to its students with the ability to access any information, from any

(See "Theme" on Page 21)

Also In This Issue:

CEDPA Board of Directors

President
Warren Williams, Assistant Superintendent,
Information and Technology Services
Grossmont Union High School District
P.O. Box 1043, La Mesa, CA 91944
(619) 644-8199 FAX: (619) 462-7420
e-mail: wwilliam@guhsd.net

Past-President
Darryl La Gace, Director of Information Services
Lemon Grove School District
8025 Lincoln Street, Lemon Grove, CA 91945
(619) 589-5600 FAX: (619) 461-4539
e-mail: dlagace@lgsd.k12.ca.us

President-Elect
Scott Sexsmith, Information Systems Manager
Merced County Office of Education
632 W. 13th Street, Merced, CA 95340
(209) 381-6693 FAX: (209) 381-6776
e-mail: ssexsmith@mcoe.merced.k12.ca.us

Secretary
Jane Kauble, Staff Services Manager, ITS
Los Angeles County Office of Education
9300 Imperial Highway Downey, CA 90242-2890
(562) 922-6141 FAX: (562) 803-8957
e-mail: Kauble_Jane@lacoe.edu

Treasurer
Judy Acosta, Support Services Manager
Ventura County Superintendent of Schools
5189 Verdugo Way, Camarillo, CA 93012
(805) 383-1954 FAX: (805) 383-1997
e-mail: acosta@vcss.k12.ca.us

***DataBus* Editor**
Addison Ching, Director, Information Dissemination and Access
California State University, Office of the Chancellor
401 Golden Shore, Long Beach, CA 90802
(562) 951-4290 FAX: (714) 968-9574
e-mail: aching@calstate.edu

Directors
L. Russ Brawn (2001), Information Systems Administrator
California School Information Services
770 L. Street, Suite 1180, Sacramento, CA 95814
(916) 325-0887 FAX: (916) 325-0858
e-mail: rbrawn@csis.k12.ca.us

Mike Caskey (2002), Director of Information Systems
Stanislaus County Office of Education
1100 H. Street, Modesto, CA 95354
(209) 525-5085 FAX: (209) 567-4365
e-mail: mcaskey@stan-co.k12.ca.us

Oswaldo Galarza (2002), Director, Information Services
Orange Unified School District
1401 North Handy Street, Orange, CA 92867
(714) 628-4100 FAX: (714) 744-3796
e-mail: galarza@orangeusd.k12.ca.us

Terrell Tucker (2001), Director, Information and Technology Services
Panama-Buena Vista Union School District
4200 Ashe Road, Bakersfield, CA 93313
(661) 831-8331 x144 FAX: (661) 398-2141
e-mail: tt@pbvusd.k12.ca.us

SIG Chairperson
Greg Lindner, Director, Information Systems
Elk Grove Unified School District
9510 Elk Grove-Florin Road, Elk Grove, CA 95672
(916) 686-7710 FAX: (916) 686-4451
e-mail: glindner@edcenter.egusd.k12.ca.us

CEDPA Information

CEDPA is an association of K-12 Technologists. Founded in 1960, the major emphasis of the association's activities are directed towards improving K-12 Technology in public education within the State of California and to prepare its membership to better meet and support the technological needs of Administrative and Instructional Programs.

CEDPA is a California non-profit corporation, as recognized by the Internal Revenue Service.

As cited in CEDPA's bylaws, the purpose of this organization shall be:

(a) To provide information to the California public educational community concerning educational information systems and technologies via dissemination at an annual conference, through quarterly periodicals and special seminars.

(b) To foster the exchange of knowledge of educational information systems and technologies concepts, systems and experiences between local education agencies and other associations both at the state and national level.

(c) To inform the association membership of important information concerning educational information systems and technologies.

(d) To provide recommendations to the State Department of Education, State Legislature, school districts, county offices of education and other public educational organizations concerning educational information systems and technologies.

(e) To develop professional standards for the educational information systems and technologies community within the State of California.

Yearly membership in CEDPA is granted to attendees of the Association's annual conference. Individuals interested in the Association's mailings may request to be added to CEDPA's mailing list by writing to the address below or filling out the interest form at CEDPA's website.

The *DataBus* is published bimonthly by the California Educational Data Processing Association and is distributed without charge to all members of the association and other selected technologists within the State of California who are interested in information systems processing and technology in K-12 education. Submissions, correspondence, and address changes should be sent to the editor at:

CEDPA
P.O. Box 6552
Huntington Beach, CA 92615-6552

Electronic editions of the *DataBus* and information about CEDPA are available from CEDPA's website at
http://www.cedpa-k12.org

President's Column

Developing Our Web Pages To Better Serve the Membership

Warren Williams, Grossmont Union High School District

In the last President's Column, I talked about the organizational effort required to produce a conference that would meet the needs of each attendee. The annual conference is but one of the many benefits that are provided to our membership. I would like to take this opportunity to discuss two more benefits that will be developed this year to assist our members in the performance of their job responsibilities. I plan on working very closely with Addison Ching to expand the web presence of CEDPA. We have discovered that our electronic world is assuming a much larger role for us than even we anticipated. We have tried rather unsuccessfully for the past three years to generate attendance at our Special Interest Group (SIG) meetings and with little success. Our suspicion is that the web has replaced the SIG meetings as a more personalized way to gather information. I regret loosing the networking and information sharing that happened at SIGS. I also enjoyed the opportunity to meet again with friends from around the State, but realize that taking a full day from work is difficult for many. To fill in the information gap resulting from the loss of SIGS, the Board of Directors has authorized the fuller development of CEDPA's web presence.

First and foremost, we will organize a Job Center. The center will contain a number of features. It will afford to members the ability to post job openings for technology positions. We will maintain the posting until the position is filled or the expiration date is reached. An archive will also be maintained in case the job is again vacated. The posting will contain all of the information usually associated with a position including district information, hours, pay, duties, reporting details, contact information and any other relevant facts you would care to list. The postings will be searchable and will also be organized by the various classes of jobs within our organizations. Posting will be done through a browser-based form and will require proof of membership (info on this coming in another column).

The second component of the Job Center will be a database of job descriptions. Once again we will provide these in a searchable format and organized around job types. These descriptions will probably be available in pdf and MS Word format. We will attempt to bring some uniformity to the postings so that they can be compared. As an outgrowth of this function, I hope to have a salary comparison table developed. This should be most useful given the competitive nature of our industry today. It should also be helpful in negotiating for salary adjustments for positions within your organizations.

Finally, I would like to see an area in the Job Center for assistance for applicants or for managers who are seeking applicants. In this area there might be tips on resume writing or at least a list of sites that offer this service. We could post a short synopsis of current trends in the industry as they relate to job designs. There should be a Human Resources area that will list opportunities for training to keep current, perhaps even some suggestions on how to alleviate stress on the job. There are many avenues we can take in this design.

As we use the web more frequently to communicate, CEDPA will use its web presence to organize information to facilitate that communication. We already have listservs that are used by many in the educational technology community. The next iteration of the listservs will maintain the electronic dialog in a searchable archive so that members can get to information that was posted previously. This should be helpful in gathering information on topical issues as they present themselves to you. When processing erate applications, a feature like this could prove invaluable. It will help in the review of comments on various student or financial packages. It can even help with contact information for various issues or practices.

Another particular area that would be most helpful would be one that maintains information on bids. There are many facets to bid preparation and CEDPA will attempt to organize this process in a manner that facilitates the development of bids. Maybe we can call this area Bid Central. There will be a database of bids that have already been posted. This will provide the member with language that can be used for bid writing. We hope to begin developing consensus about writing bids so that others might piggy-back on well developed bid packages. If we are really successful, we might even help to develop consortia to leverage our purchasing power. Certainly at

(See "President" on Page 28)

Spotlight on Technology: The Environmental and Spatial Technology (EAST) Grant

Joyce Hinkson, Ed.D., California Department of Education

California has joined in the effort to change the face of technology, one site at a time. What began as one teacher's idea to assist at-risk students has grown into a grass-roots effort that now encompasses over 150 schools in six states. This month, meetings were held in two California cities for the finalists and semi-finalists of the competitive Environmental and Spatial Technology (EAST) grant. Grant finalists will receive a total award of $125,000 per year for at least two years to implement this grade 9-12 project. Both the ten finalist sites and the six semi-finalist sites received sufficient funding to attend the pre-implementation workshops in California and to also attend the EAST conference in Little Rock, Arkansas on February 19-21, 2001.

The EAST model is a dynamic, performance-based learning environment for students utilizing project-based service learning, integrated with advanced technological applications. The setting for this model is an interdisciplinary laboratory environment where the intellectual and problem-solving growth of students, rather than technology, is the focus. Technology is a tool integrated into the learning process; it is not taught as a separate entity. Students learn in a non-traditional environment that may include being out of the classroom and or lab to gather information and do research on a regular basis. Soft skill sets such as effective communication, collaboration, problem-solving and teamwork are nurtured. As part of the hardware and software package for EAST, sites will receive advanced technology workstations, printers, a plotter, and other peripherals. Software will include technical applications from architecture, animation, database development, 3D design engineering, digital imagery, electrical design, global positioning, geographical information systems, image analysis, publishing, visualization and web development. As with any comprehensive program, a key feature of EAST is the staff development component for the teacher/facilitator. EAST provides up to 23 days of training in the first year of implementation.

This past week, I felt fortunate to travel with a group from the national EAST project and give pre-implementation workshops in San Diego and Redwood City. I watched closely as Arkansas students enrolled in the EAST program confidently presented their technology projects to a group of approximately 50 California superintendents, principals, teachers, counselors and technology coordinators. Presentations were varied and included assisting firefighters locate fresh water sources for extinguishing brush fires in Hawaii, designing and painting a mural to brighten a county health facility, building a Newtonian telescope and locating suitable areas for a helicopter landing pad to rescue fallen hikers. Even though the projects were inspiring, the EAST directors made it clear to the audience that student projects were focused on the process, rather than the product.

EAST has generated a lot of interest and excitement among educators who have seen how the project positively impacts students. California's first round of competition funded ten demonstration sites throughout the state. A second competition round is planned to fund even more sites. Information about the grant may be obtained from the California Department of Education's web site: www.cde.ca.gov/east.

Student Technology Showcase

The California Department of Education will sponsor the first statewide Student Technology Showcase to highlight curriculum-based student technology projects from grades 4-12. Students will have the opportunity to present their projects to an audience that will include parents, teachers, administrators, higher education representatives, California Department of Education employees, California Technology Assistance Project members and legislators or their representatives.

The Student Technology Showcase will feature exemplary student projects that may include, but not be limited to, web video, multimedia, graphic art, sensor/probe data and analysis, animation, or database development. This will be an excellent staff development opportunity for teachers and others to see effective integration of technology and the curriculum throughout the state.

The event will be held on March 5, 2001, in Sacramento and admission is free. See http://www.cde.ca.gov/showcase/ for more information and registration.

Dr. Joyce Hinkson is a consultant for the California Department of Education's Education Technology Office. She may be reached at (916) 323-2241 or by e-mail at jhinkson@cde.ca.gov.

Recent Legislative Updates

Greg Lindner
Elk Grove Unified School District

Children's Internet Protection Act

Internet Filtering will now be required to receive Erate funds or Federal funds.

> *"President Clinton signed into law the Children's Internet Protection Act on December 21, 2000. That law, attached to the omnibus appropriations law during the last days of the 106th Congress, will require schools and libraries that receive funding under either Title III of the Elementary and Secondary Education Act or the Museum and Library Services Act, or that receive universal service discounts for Internet access ("E-rate") to adopt an Internet safety policy incorporating the use of filtering or blocking technology on computers with Internet access.*
>
> *"Section 1721 applies to schools and libraries for computers with Internet access as a condition of receiving discounts from the Universal Service Fund. (Recipients of discounts for basic telephone service are excluded.)"*

(Excerpts from http://www.sl.universalservice.org/whatsnew/CIPA020101.asp.)

Another summary of this new federal law can be found at http://www.cde.ca.gov/erate/e-ratehr4577.pdf. The summary was put together by Van Wilkinson for a presentation to CCSESA. Basically, the law states that if you want to continue or start to get Erate funding, you better get a filtering policy in place. The law states that the protection measures must be in place by October 1, 2001 (120 days after the start of the next funding year).

If you haven't heard about this you need to read Van's summary or the SLD summary.

Additionally, if you would like to comment on the FCC's interpretation of the law and their implementation of it you can do so as described below from the Universal Services Web Page (http://www.sl.universalservice.org/whatsnew/default.asp#020101)

The Notice of Proposed Rule Making adopted by the Federal Communications Commission on the implementation of the Children's Internet Protection Act (CHIP Act) has been published in the Federal Register on January 31, 2001.

The notice can be found on pages 8374-8377 of the Federal Register, Vol. 66, No. 21, for Wednesday, January 31, 2001. It is available on the web in both text and PDF versions as the only entry under the "Federal Communications Commission" heading on the <u>Federal Register</u> (http://www.access.gpo.gov/su_docs/fedreg/a010131c.html) web site.

Comments are due on or before February 15, 2001. Reply comments are due on or before February 22, 2001. Addresses for filing comments are available under the heading "ADDRESSES" at the beginning of the notice.

AB2882

The Education Technology Grant Program for High Schools (AB2882) will provide $175 million in grants to eligible school districts and charter schools. The goal of the program is Advanced Placement but also lowering the student to computer ratio. It will provide $1500 per computer to lower the ratio to eligible schools, funding permitting.

The following is now available on the Office of the Secretary of Education's Web site. Official letters to Districts were mailed the middle of January. http://www.ose.ca.gov/edtech/index.html

There are specific rules that must be followed with this program. In a nutshell, the funding is sent to the district and the district purchases the computers. There are strict guidelines on what can be purchased (minimum standards). $1500 has been allocated per computer. Districts are allowed to use any difference of what it costs to buy the computers and the $1500 to purchase more computers or to purchase the necessary infrastructure to get the equipment on the network. Districts are also required to take an assurances page to their board for approval. Charter Schools must have the Director sign the assurances page.

The funding must be encumbered by June 30th. The machines do not have to be installed until the following year.

What is the remaining timeline?

January	Put a placeholder item on your Governing Board agenda to accept funds, agree to assurances
3/1/01*	Those receiving awards must have a technology plan on file

(See "Legislative" on Page 9)

Scheduled CEDPA Conferences Promise Return To Favored Venues

Russ Brawn, California School Information Services

Year-by-year, each of us in technology determinant fields seems to be driven to shorter timelines, tactical reaction, and near-term planning. The pace of change challenges us as it becomes more and more difficult to anticipate policy swings, product offerings and 'lightning rod' issues. Still, one responsibility you may have in your home district or county office is to keep an eye on the horizon, anticipating long-term needs beyond the present and next years. Your CEDPA Board faces a similar mix of near term and long term planning in anticipating membership needs. Given all of the above it is very gratifying to have long term commitments in place for future conference facilities – to be able to 'hang our hats' on something as far as four years away.

Good space is hard to find, and even harder to arrange into a schedule which will comfortably fit into the school year at a rate which our strained public education budgets can afford. An added complication is that, even with our recent extraordinary growth in conference attendance, our space demands continue to be a bit out of the norm. We're a focused group with a regional (as opposed to national) membership that limits the number of attendees, yet the support we enjoy from the vendor community demands extensive exhibit space. As a consequence, facilities to which we are attractive are somewhat limited and fill up *fast*.

About that 'recent extraordinary growth' — the Santa Barbara Conference was our highest attended ever, both by we K-12ers and by vendors. The previous records for both members and vendors were set in Monterey, 1999 and the data are that the attendee numbers were only approached by the Monterey, 1989 Conference. Growing technology challenges and budgets certainly have a lot to do with the last few years of growth. But the importance of a suitable, comfortable venue encourages each of us to expend the effort necessary to catch up so that we are able to break away. The result is that California's community of educational technologists has a yearly window to explore possibilities and find solutions to those forementioned short-term urgencies and long-term directional setting.

We are very pleased to announce that the CEDPA K-12 Technologists Conference will return to the Fess Parker DoubleTree Resort in Santa Barbara. Not for just another year, but for both 2003 and 2005. Not only were we happy, the resort staff and administration were impressed with the quality of the program and by the demeanor of all of us. Apparently, none of us took too many towels, trashed the putting green, or broke anything that couldn't be easily repaired.

This year we return to Monterey and the same exceptional DoubleTree venue as in 1999. We are getting the largest room block available, but make sure to get reservations in early. We extended to multiple adjacent facilities our last time there. Note that we are returning not only to the hotel, but hope to return to the Carmel Valley Ranch, one of the better golf courses hosting a CEDPA tournament. The following year, we return to Palm Springs, the city that so many of us enjoyed in 1996 and 1998. The 2002 venue is new to us, however, as we settle in at the beautifully refurbished Riviera Resort & Racquet Club. The 'Riv' has been a splendid attraction to many notables over the years. Do the names 'Marilyn', 'Elvis', or 'Frank' evoke memories?

As you review the following table you may observe a couple of things. An obvious point is that the site for 2004 is undetermined. *We welcome your advice* on cities and sites, whether a return to a favorite locale or something new for CEDPA. As you consider options, you may observe a second item – after forty years, we have diverged from our 'odd years in the North, even years in the South' scheduling dictum. Part of that decision was driven by the opportunity to lock in Santa Barbara for those two, available years. Another factor is recognition that California is a 'tall' state – that while Santa Barbara is definitely SoCal to us NorCal folk, it is still several driving hours from other southern cities. So some rotation

(See "Venues" on Page 7)

2001 CEDPA Conference
November 14-16, 2001
Doubletree Hotel
Monterey-Fisherman's Wharf
Monterey, California

See http://www.cedpa-k12.org/2001Conference/

CEDPA SIGs Sail Off Into The Sunset???

Mike Caskey, Stanislaus County Office of Education

"The time has come," the Walrus said,
"To talk of many things:
Of shoes—and ships—and sealing-wax—
Of cabbages—and kings—
And why the sea is boiling hot—
And whether pigs have wings." Lewis Carroll, 1872

Lewis Carroll wasn't talking about CEDPA SIGs when he wrote "Through the looking glass….", but he does sort of capture the essence of the transformation of CEDPA SIGs. On the other side of the looking glass, Alice found a different world. Things looked and acted differently from her former frame of reference.

So it is with the CEDPA Special Interest Groups. They have become a little used forum for K12 Technologists to share ideas, commiserate on common problems, and help one another gain a clearer vision of the future of California K12 technology. In fact, the SIG meeting at the conference managed to attract only one individual.

As discussed in previous DATABUS articles, your CEDPA Board has reviewed and discussed the SIGs, and their continued viability, at great length. And, after great soul searching and agonizing, the Board has come to the conclusion that the SIGs no longer provide a good vehicle for the type of information exchange needed in our rapid paced environment. Two current thoroughfares for this exchange are e-mail and the CEDPA EdTech listserv. Also, many County Offices of Education host regional meetings, which serve as forums for the exchange of information.

The next step??? The proposal that has gained the greatest amount of support from CEDPA Board members, is the concept of a 1-day "mini-conference" to be held approximately in the middle of the CEDPA calendar-about 6 months prior to the annual 3-day conference. Such a "mini-conference" would have an abbreviated speaker program and would most likely be focused on one or two topics. As envisioned, this one-day event would include both morning and afternoon sessions and most likely, a "working" lunch where the attendees could participate in small or large group discussions on "the topic of the day".

Just as Dorothy and Toto found themselves no longer in Kansas, so the CEDPA SIGs find themselves no longer in the real world. But, the CEDPA Board is not looking for Wizards to help SIGs find a way "home". I'm sure you've guessed what's next.

What do you think? Would you be interested in attending such a 1-day function? Would you recommend some other type of CEDPA function to help the membership with their ongoing pursuit of K12 Technology excellence? Greg Lindner has been given the unenviable task of rebuilding the SIG program into one of vision and use for you, the members. Please contact Greg at glindner@edcenter.egusd.k12.ca.us and share your ideas with him.

Venues

(Continued from Page 6)

of sites among south, north, and something akin to 'in between' is not unreasonable.

For your near term planning and long term visioning, here are dates to remember:

Year	***Date and Location***
2001	November 14-16, Monterey Doubletree Monterey-Fisherman's Wharf
2002	October 16-18, Palm Springs Riviera Resort & Racquet Club
2003	November 19-21, Santa Barbara Fess Parker DoubleTree Resort
2004	To be determined
2005	November 17-19, Santa Barbata Fess Parker DoubleTree Resort

Any suggestions for the 2004 Conference location or feedback regarding past sites should be forwarded to Russ Brawn, email rbrawn@csis.k12.ca.us.

California Takes the E-Rate

A Summary of E-rate News and Events

Van Wilkinson, California Department of Education

The times (they are) a changin'

These are the times of change with several large-scope education technology initiatives, federally with E-rate and Internet filtering, and, in California, with several telecommunications items that may involve the California Public Utilities Commission (CPUC). By the time you read this, some will have been more clearly resolved.

E-rate

The end of the Year 4 filing window for the notorious Form 471 closed January 18. Preliminary reports from the Schools and Libraries Division (SLD) personnel who administer the federal E-rate program are that more Form 471s were received than in Year 3. When the tallies are released, we will have some idea how much of the "priority one" funding (telecommunications and Internet access) has been requested, thereby giving us a rough idea of how far down the discount scale the "priority two" funding may go (internal connections). Speculation says that applicants who are not at or very near the 90% discount level may not see internal connection funding in Year 4.

At the SLD, the arrival of a new presidential administration is causing anxieties. The E-rate program just underwent an audit / inspection by the General Accounting Office (GAO), and the results were not unexpected — general approval, but weaknesses in the accountability aspects. Various proposals to revamp the E-rate program are now being released and debated. If the E-rate program is combined into other existing federal funding channels and/or into a state-level block grant type allocation, it will mean a radically different E-rate program. The public school sector plus unexpected allies (nonpublic schools and telcos) appear to be generally united in support of retaining the program, if not in its present form, then at least in a manner that does not cause current recipients to find their network connectivity soon unaffordable.

Internet Filtering and E-rate

HR4577 mandates Internet filtering and other supervisory steps for those receiving federal funds (ESEA, E-rate). The California Department of Education (CDE) has a website, maintained by the Education Technology Office, with a graphical overview of the filtering issue plus an annotated version of the full law (www.cde.ca.gov/erate, under "News" go to "Current").

Estimates are that about 60% of public schools have some type of filtering in place, but since filtering is <u>not</u> an eligible service under current E-rate rules, Year 4 applicants presumably did not apply for discounts on that service. Yet, some did, either inadvertently or gambling that it would become eligible. The Federal Communications Commission (FCC) has released tentative material relative to the Internet filtering law for public comment, and they are to have finalized their rules by April 20, during the period that the first "waves" of E-rate funding commitment letters begin to arrive from the SLD. October 28 is the generally recognized last day for E-rate recipients to certify compliance with the new law (120 days after the "first" program year, which is E-rate Year 4, starting July 1). Complicated? Yes. Will it change between now and then? Probably.

CPUC may assist on some old and new issues

The California Public Utilities Commission (CPUC) or its staff may be looking into several issues affecting public K-12 telecommunications deployment and billing. One is the appearance of "911" charges on telephone bills paid by public K-12 schools; we may be exempt from these charges. Another may be the related matter of exemption from most taxes and some surcharges on telephone bills. Check your bills. If you see excise tax or local (municipal, city) taxes on the bill, it may be appropriate to contact your service provider to see about the process to determine your exemption status. Most service providers routinely adjust their billing programs for public K-12 when services are ordered, but it is not a 100% surety.

The California Teleconnect Fund (CTF), California's E-rate sibling, does not currently provide the 50% discount for services above the DS3 level, but Pacific Bell has submitted a request to the CPUC for that to occur. If this is approved (it would presumably apply to all service providers), those needing bandwidth in larger amounts would be able to save considerably (50%) for these recurring charges. One question will be whether inclusion of such costly circuits will have an adverse effect on the CTF funding pool.

(See "E-rate" on Page 9)

E-Rate

(Continued from Page 8)

In an attempt to bring some order to what is widely regarded as an unacceptable situation regarding reconciling E-rate and CTF discounts “stacked” together on telephone bills and reports, many cooperative efforts are underway to arrive at a statewide standard. Some E-rate recipients who have been audited by the SLD have simply been unable to verify how and when certain discounts are being applied, even with extensive help from their telco. Within the telco community, different service providers are taking different approaches, but California stands alone in the way it concurrently and retroactively attempts to account for simultaneous (E-rate and CTF) discounting.

Van Wilkinson is with the California Department of Education Educational Technology Office. He may be reached at (916) 323-4709 or by e-mail at vwilkins@cde.ca.gov.

Receive the latest E-Rate information and updates by joining CEDPA’s E-Rate Listserv.

CEDPA Listservs

As a service to K-12 Technologists, CEDPA hosts several e-mail discussion distribution forums (listservs) on various technology topics. These lists are open to anyone with an interest in the topic area.

Edtech - A discussion forum for educational technology issues.

Erate - A discussion forum for E-Rate, the FCC ruling on Universal Service that provides schools and libraries significant discounts on telecommunications services.

To join a distribution list, send an e-mail message to listserver@cedpa-k12.org. Leave the message subject blank. The message body should contain only two words: the word **subscribe** and the name of the discussion list you wish to join. The rest of the message should remain blank. Do not append your signature line or any other text to the message.

To leave a list, send a message to listserver@cedpa-k12.org as above, except use the words **unsubscribe** and the name of the list you wish to leave.

Exhibitors Wanted

Oswaldo Galarza
Orange Unified School District

The **41st Annual CEDPA Conference** is scheduled to take place November 14th, 15th, and 16th, 2001 in beautiful Monterey California, at the Doubletree Hotel Monterey-Fisherman’s Wharf. The conference theme is “Education: The Digital Future”.

The CEDPA vendor show is one day only, November 15th and offers dedicated time for our vendors and attendees to meet with each other. No breakout sessions are scheduled during the Vendor Show. We have **sold out** the last three years with vendors scrambling to make special arrangements at the last minute.

Sign up early! A vendor registration form can be found elsewhere in this issue. Complete and mail, fax, or e-mail it to me. Visit CEDPA’s Web site www-cedpa-k12.org to get more information or to download the vendor registration form. Feel free to contact me at 714 628-4152, or by email at galarza@orangeusd.k12.ca.us.

CEDPA looks forward to your participation. For those of you who have been with us in the past, we have expanded (duplicated) the vendor show area and are expecting to offer 68 10x10 booths and 5 Kiosks (20x20 Island booths) at the Monterey Conference Center.

Legislative

(Continued from Page 5)

6/30/01* Eligible schools/districts must encumber funds to purchase computers

Fall 2001 AP Online classes must be offered (for those who accept Priority One funds)

Fall 2001 We ask for, though do not require, installation of Priority Two and Three computers.

3/1/02* Eligible schools/districts must complete installation, submit completion form to CTAP, and update online inventory.

6/30/02* CTAP compliance visits completed, report to Secretary for Education

* These dates are set in statute or regulations.

Conference Central

A behind-the-scenes look at preparation for the fall conference

Scott Sexsmith
Merced County Office of Education

Planning. Hours of it. That's what it takes to try improving upon the spectacular conference we had last year at the Fess Parker Resort in Santa Barbara. Mark your calendars now for the 2001 CEDPA Conference November 14-16, 2001, that will be held at the Doubletree Hotel near Monterey's Fisherman's Wharf. As many of you will remember, this was also the site of our 1999 conference.

This year the conference theme will center on the future of digital education in California. The Digital California Project is coming at all of us this year as the first round of DCP node sites will be installed throughout the state. Connectivity of all schools to the node sites will certainly be a timely topic at the conference. CEDPA Director Mike Caskey will be organizing the speaker strands to address this issue as well as others.

Director Oswaldo Galarza will be responsible for developing the vendor show this year. The vendor show area will be twice as large as it was the last time we were in Monterey, and the number of vendors participating continues to grow each year. We're exploring the possibility of increasing the size of booths to give vendors more room to show their wares this year also.

The Network Operations Center (NOC) will be under the watchful eye of Terrell Tucker. While this is always the place at the conference to see the latest networking gear, Terrell has plans to reorganize the NOC a bit from prior years. I think you'll be pleased with what he has in mind. We're also going to be incorporating the list of NOC "tech-talk" presentations with the other speaker strands on a "super" conference overview sheet that attendees can use to quickly find what's happening during any given time at the conference.

We hope that you've already marked on your calendar this upcoming conference. As always the conference is a great place to get together with your peers, discuss common issues, learn from each other, and to find out what works and what doesn't. In Monterey this year you'll also get to see what promises to be our largest vendor show ever. I'm very interested in what ***you*** have to say regarding what we can do to make this a great conference! ***Please*** e-mail me at ssexsmith@mcoe.org with any comments or suggestions.

2001 Call for Speakers

Mike Caskey
Stanislaus County Office of Education

CEDPA is in the process of developing its 2001 Fall Conference program for breakout sessions. Your participation will contribute to a successful conference. If you have a topic you would like to present to our attendees, please sign up! This is your opportunity to share your experiences and lessons learned with your successful (or not so successful) hardware or software implementation. Please reserve your place early as we would like to have the conference program for breakout sessions developed and published with the Conference Announcement in July.

We are especially interested in your experiences with the following topics:

- Administrative systems migrations(student or financial systems)
- E-Rate experiences
- Network connectivity
- ATM or gigabit Ethernet implementation
- VPN Deployment
- Windows or Novell networking
- Emerging technologies
- Help desk support
- Data mining and warehousing
- Firewall design and implementation
- Intranet / Web development
- Instructional technology (with the exception of curriculum)
- Windows 2000
- Wireless technology

A breakout session typically lasts for 45-55 minutes and can seat up to 50 conference attendees.

A Call for Speakers form is included in this issue of the *DataBus*. The form is also posted at www.cedpa-k12.org in PDF format. You are encouraged to sign up as early as possible. Please complete and send your forms via postal mail, fax or e-mail to:

E-mail:	mcaskey@stan-co.k12.ca.us
Fax:	(209) 567-4365
Voice:	(209) 525-5095

Best Practices – Anti-Virus Strategy Guide

Contributed by Jed McNeil & Lisa Milburn, Network Associates, Inc.

Computer viruses have become a ubiquitous feature of modern computing. New major virus threats like the Melissa, W32/ExploreZip.worm, and most recently, the LoveLetter virus, are appearing on an all too frequent basis. These viruses can all have effects on your PCs (being rogue applications interacting with your machine) and business, ranging from employee downtime, user distractions, and add to the workload of the help desk. An anti-virus solution that limits the mischief that these viruses can cause is therefore a necessity.

Anti-Virus software is as complex as any enterprise application to install and rollout to a large user-base. Unfortunately, Anti-Virus software requires regular updating to be effective. At this stage, most vendors offer weekly updates, but there is already a requirement growing from industry for daily and even hourly updates.

The 1999 ICSA Virus Prevalence Survey provides some astonishing data, "over 4/5ths of respondents claimed to have at least 90% coverage of PCs with anti-virus protection." Yet very few of the same respondents had anti-virus protection installed and active at the mail and gateway levels.

Furthermore, although many networks have anti-virus software installed, this does not mean that they are prepared to respond effectively in the event of a virus outbreak. Within many organizations, it is common problem to see desktops and servers with a lack of up-to-date anti-virus protection. Some common challenges contributing to this problem include: conflicting programs, inefficient or inoperable distribution processes for new, critical DAT files, no clear anti-virus policy, or over-utilised IT resources.

McAfee, a Division of Network Associates, Inc. is a company that is uniquely qualified and committed to assisting companies with the successful implementation of the industry's most effective enterprise anti-virus protection. The first step in this endeavor is to create an effective anti-virus strategy. Thus, the purpose of this document is to help you recognise the current virus threats you face, and to create an appropriate anti-virus strategy to counteract these virus threats.

When reviewing this guide, you should first consider the following qualifying questions:

1. Do you consider viruses to be a threat to your organization?
2. Do you use and share electronic data?
3. Do you have an anti-virus strategy, identifying what the virus threat is to your business and the policies and procedures to protect your data from virus infection, corruption or deletion?
4. Does the strategy include concepts such as these?
   - A policy defining what products are installed, how they are configured and maintained.
   - A method for implementing the policies in your infrastructure.
   - A policy and associated procedure for dealing with virus outbreaks.
   - Documentation of the strategy to allow any member of your IT team to manage your anti-virus tools.
   - Procedures and guidelines for users.
5. How do you assess the effectiveness of your anti-virus strategy?
6. When did you last review your anti-virus strategy? Does it reflect the current threat, the trend of viruses that propagate via e-mail and the web, and changes in your IT infrastructure?

If you don't have answers to the above questions, then read on, as the next several pages will get you on your way to creating an effective anti-virus strategy for your organization.

Identifying the threat

Before you create your anti-virus strategy, you must first review your working environment. That is, to be able to protect against the virus threat, you must first understand the threat to your organization.

For example, a single home user with a dial-up ISP web connection, faces a very different threat to a corporate business. Home users need protection against the data they download from the web, e-mails they send and receive, and the media they use in the PC. For most, the effects of a virus are annoying and time-consuming, but do not result in revenue loss. The corporate business often relies on the data such as customer information and records to help them create revenue. This important, and often critical data, is the reason for anti-virus protection. If the data is lost or corrupted, business revenue is directly affected. As such, the need for protection is essential and the possible sources of infection increase with the size and detail of their IT infrastructure.

(See "Anti-Virus" on Page 12)

Anti-Virus

(Continued from Page 11)

How do I identify the threat?

So, having understood the need to quantify why we need to protect, you should ask the following questions:

1. How can a virus enter my organization?
2. Where can a virus be stored within my organization?
3. How can viruses be transferred or replicated around my organization?
4. Where does a virus get triggered within my organization?

The next sections explain the common threats that we have seen in the different levels of organizations.

Small enterprise

Physical Media - Still used in virtually every business, whether it be the traditional floppy disk, through to Jaz drives, optical disks and CD-ROMs. These all contain data that could be virus-infected and so virus scanning is required. The strategy decision is whether to rely on the desktop anti-virus software to either proactively scan the media using an On-Demand scanner, or rely on the On-Access scanner to pick up infected media as its used. Traditionally many businesses have followed a procedure, such as passing the media to IT support to be scanned using a stand-alone dedicated machine known as a footbath or sheep-dip. These normally have one or more anti-virus products installed and some simple menu to allow staff to check the media. Some companies (such as many government agencies) also have such machines in reception, and request all visitors to scan any media they bring on site prior to usage at the PC. Beyond its physical ability to act as a front line of virus defense, the footbath or sheepdip machine also acts in this instance as a marketing tool, showing the company to be a virus-aware and security-conscious organization.

PCs - Traditionally still the backbone of most virus outbreaks, the workstation is the location that most viruses are triggered and replicate. We will focus later in this document on the policies used to protect the user's machine.

Servers - These offer a dual threat in terms of virus outbreak. Firstly the servers in your organization normally contain your mission-critical business data. As such, they should be considered as the core of your anti-virus protection strategy. In most instances, this is the most important data to the business and should be backed up on a regular basis. Secondly, most servers also act as the data communication hub for the workstations. So servers also lend themselves to the threat of being a virus storage and transfer mechanism. This means when looking to protect your server, you should consider carefully protecting not just the long-term data stored, but also the connections made to the server from networks or other forms of remote node.

Dialup ISPs (web and e-mail access) - From the small single-node business to global corporations, most have users (often with laptops) that have modem dialup accounts to ISPs. These offer their own unique virus threat on two levels. First, they allow the user to gain access to public e-mail and the web, via a method outside of the corporate standard. This means they fall outside the general considerations of the protection strategy. Most corporations will funnel users through a single point of access to the web which can be controlled by a firewall and scanned with the appropriate anti-virus software. The dialup ISP offers a method to circumnavigate this protection. Second, they offer access to known shortcuts for communication such as Hotmail Internet mail. We have seen instances when normal corporate mail has been disabled due to a virus outbreak, and users have then turned to these other forms of communication, which may also be an everyday entrance "hole" for viruses into your network.

Medium Enterprise

Laptops - Common to virtually every organization, these are probably the hardest resource on which to maintain an effective level of virus protection. Because they are portable, they are very open to infection. It is common practice to take these onto other customer/client sites. And there is an increased temptation to share data as the users are outside the physical restraints and control of their own organization. Add to this, most laptop users today will have Remote Access Server (RAS) access to their corporate mail account and in many instances the corporate network, they pose not only a threat to themselves but also a threat to your network. Generally there are two main approaches adopted to protecting laptops.

1. Primarily the solution is to give them strong all-round anti-virus protection (that is, On-Access scanning and On-Demand scanning against all forms of data transfer,

(See "Anti-Virus" on Page 13)

Anti-Virus

(Continued from Page 12)

such as e-mail, web access and file access). The difficulty with this can come with the maintenance of the software. You need a web-based form of update that is small and simple to apply, using the client anti-virus software. Where you can not gain updates from the web, many still send physical updates out to laptop users, however these can take time to reach the users, and regular updating can become costly.

2. The alternative solution is to treat the laptop as a unknown quantity within the business. This still means providing best endeavors of anti-virus protection, but ensuring before the laptop users can gain access to the main network, their machines are checked for viruses using the latest versions of anti-virus software (often triggered via a login script). Or this means controlling what access they have to the LAN, and ensuring the data on that segment of the LAN is well protected against being infected by the laptop user.

Remote Users - Although the access to media from other organizations is not prevalent, they again work outside of the physically controlled environment and can again be a greater threat to the business than your standard local networked users. When looking to add remote users to your anti-virus strategy, you should consider them in the same light as the laptop user.

WAN links - Much as the local server, these act as key flow points of data between segments of the LAN. When reviewing the virus threat and your anti-virus strategy, these should be considered for two reasons. Firstly in instances of file-based virus outbreaks these can act as flow barriers limiting how far the virus can spread. Secondly they offer a key point of protection, that requires little effort to maintain.

Corporate e-mail and web access - The '99 ICSA Virus Prevalence Survey defined over 50% of all infections outbreaks as being e-mail-based. And we suspect that about 80% of virus infections are now e-mail or web related. This has been the result of two changes. Firstly we all now use both mechanisms for sharing files specifically Microsoft Office documents. Again the ICSA report accounted for 2/3rds of all virus outbreaks being macro-based. Secondly we have seen the instigation and rapid growth of viruses that proactively use MAPI mail to replicate themselves around the organization, by grabbing user information from the address books and sending infected mails using VBS scripting. To date, this is probably the weakest point of most organizations anti-virus strategies, with many organizations failing to recognize and/or address this threat. This highlights why regular reviews of your anti-virus strategy are so important. Many organizations rely on the desktop protection to protect against this threat, which is ill-advised. First, this relies on all workstations being covered with up-to-date anti-virus software. In other words, a single line of protection must be 100% consistent to be effective. Multi-layered defense gives the cross-cover where some areas may fall short of the desired level of protection.

In reality, 100% perfect desktop anti-virus coverage is an un-achieveable target. A 90-95% desktop coverage is the realistic goal you should aim to achieve. The second issue with relying on desktop cover is the fact that most mail systems are proprietary. That means your desktop anti-virus scanner must be able to understand and scan within that environment. If this is the case, you will be able to protect the users' mail, otherwise the user will still be protected against running any attachments by their on-access scanner, but they will not be able to clean any viruses in the mail system. It makes strategic sense to have a central tool local to the mail system and gateway to scan data throughput. This allows access to both scan and clean both mail, databases and web downloads for all connected users from a single source. As we will examine in more detail later, having this key point of detection can be very important both for simplicity of maintenance anddealing with outbreaks.

Alternative data storage - UNIX, DMS, backups (HSM) - Traditionally this is an area of protection that is overlooked as it is not considered live media. However the above examples, along with many others that can be found in industry, can be used to store and access data. When either running a regular virus sweep of all your media or completing a clean up these should be included. Careful consideration should be given as to how this can be achieved. Can you simply map to the device and scan all the data?

Or is there an anti-virus product that can be installed locally? When investigating this, you should be looking for an on-demand scanner and scheduler. Obviously with such devices, viruses can not be triggered so an on-access scanner is less important. You simply need to be able to scan the device to check that is not acting as a storage

(See "Anti-Virus" on Page 14)

Anti-Virus

(Continued from Page 13)

device for the virus.

Large Enterprise

Autonomous business units and the links between them - With large corporate organizations, the IT infrastructure and anti-virus strategies can often be mixed - the result of different businesses merging together or the autonomy of each unit within the business. Here each business unit may have autonomy or mixed vendors for anti-virus software. Two key concepts should be followed. First, it is important to aim for consistent levels of protection. As such, a common generic anti-virus strategy should be applied across the units, which is best implemented with the tools from each anti-virus vendor's products. This includes maintaining and updating the products with a consistent and common strategy. Second, there must be some common auditing between the units. That is, when one discovers an outbreak, they share information about the virus and how to deal with it with the other units. It is a beneficial business practice to share information about the products and levels of protection each unit has.

Shared applications and data with other organizations - Within many of today's large-scale organizations, data resources are shared between organizations (both within and outside a single company). This provides an new risk to the organization as you have a remote site that can access your network, yet you have no control or influence over their anti-virus strategy. Where such links occur, you should control the level of access they have to your network, limited to only the required data resource areas. In addition where possible, the method of communication linking the business together should have anti-virus software installed to check any data they write to your network.

Data encryption - Over the last few years, we have seen a steady growth in the use of encryption of data - from the simple password protection offered in Microsoft Office to the more advanced strong encryption techniques used in end-to-end encryption tools such as PGP and VPN network connections. All offer the same threat in terms of viruses. The data can not in most instances be scanned until it is decrypted at destination, and most anti-virus products can not identify the data as encrypted as opposed to regular scannable data. With weaker encryption, many anti-virus products can scan through the encryption. Be aware that recent versions of Microsoft Office have been using increasing stronger encryption. It is important when creating your anti-virus strategy is to understand what forms of encryption are used within your organisation, whether your anti-virus software can either scan through it or simply highlight the encrypted data. For encrypted data that can not be scanned or identified by your anti-virus product, you need to ensure the end point where the data is decrypted and accessed has the appropriate anti-virus software installed that can check the data as it is accessed.

Protecting Against the Threat

High-level anti-virus strategy

Having reviewed the virus threat to your organization, you can now start to create your anti-virus strategy to protect against it. An anti-virus strategy should be based on protection policies and the procedures required to protect against viruses. At a high level, these can be broken down into the following sections:

- Identify the data points to scan for viruses within your organization. This should include incoming data, outgoing data, and data being passed around the organization. You should be able to identify these from the threat analysis you have completed.
- Outline the anti-virus tools and their configurations that you wish to use to protect against the threat at each data point.
- Define when and what procedure should be used to maintain and update the anti-virus tools/products.
- Define the processes to be followed during a virus outbreak.
- Decide how to make users aware of the virus threat, and how to help them to deal with virus outbreaks (awareness and training).

Once defined on paper, these policies and procedures should be implemented at an electronic level..

Policies and procedures

What anti-virus tool should be used?

At each data point raised in the threat analysis, you must now review what anti-virus tools to use. In an ideal

(See "Anti-Virus" on Page 15)

Anti-Virus

(Continued from Page 14)

world, all points would have an on-access scanner installed.

The *On-Access Scanner (OAS)* is loaded automatically into memory as the operating system or resource starts. It then monitors disk or data activity, intercepting and scanning for viruses. If desired, in most instances (providing the virus is not active in memory) the scanner can clean the infection. This form of scanning has a number of key benefits. It is automated, it detects viruses in real time, and requires no human intervention to function correctly.

In addition to the on-access scanner, most anti-virus products include an *On-Demand Scanner (ODS*). This scans for viruses only when triggered, usually scanning a specific segment of data, such as a file, folder, drive or database. The benefit of the ODS is that it checks all files, not just those being accessed. As such, it is specially useful when completing a virus clean-up, by allowing you to ensure all data is virus-free. It is also commonly used to check incoming media, such as with footbath/sheep-dip techniques (described earlier in this document) or locally on the user's PC.

Within McAfee's VirusScan product, we include four different on-access scanners.

System Scan	Monitors standard file and disk activity on the PC.
E-mail Scan	Scans MAPI-based mail as received to your mailbox. Lotus Mail and Internet-based mail including HTTP and POP3 through the download scanner component.
Download Scan	Scans HTTP Web downloads.
Internet Filter	Checks for malicious Java and ActiveX, and blocks IP or URL addresses.

When would you use each of these components? In a typical networked environment, the e-mail server and Internet gateway should be protected with their own anti-virus software. As such, all the components beyond a basic system scan are providing duplicate scanning of data. This can be beneficial as cross-check scanning but should not be considered as essential to your anti-virus strategy. So, in what instances should you use these additional scanners?

In the small business model where there is no central point for mail and web downloads, each user may be connecting locally to the web via an ISP and as such the protection must be local to the user's machine. This same scenario applies in two variations to larger organizations.

First, the similar situation often applies with laptop users who have dial-up ISP accounts. Second, they may be used when for what ever reason the organization does not have anti-virus protection at the server or gateway (although this can be a less effective method).

When reviewing what anti-virus tool to use at each level, you must consider the following. Is the PC suitable to support an OAS? Most workstations are, but it is common to find both file and e-mail servers that are already suffering from excess workload, running at dangerously high utilization rates. In such cases, the ideal solution would be to upgrade that PC to deal with the workload. When reviewed in the bigger Total Cost of Ownership (TCO) picture, this is always cheaper than the cost of a virus outbreak. However when upgrading is not available, two alternatives should be considered:

- It would be unwise to load an OAS with normal scan settings (to check all possibly infectable data). This can be the metaphoric straw that breaks the server's back. As such, common sense should be used and trade-offs made, such as not scanning all data files (for example, scanning only mission-critical data). This allows the OAS to function with limited resources. When this is the case, the ODS should be run against the rest of the data on a regular basis.

- Simply rely on only on-demand scans run on a regular basis. Note that this would not stop virus infection, but would limit the period during which the virus could spread.

Where you have mission-critical data such as that stored on servers, you may wish to implement both forms of scanning - the OAS to check data as accessed, and the ODS to complete a thorough sweep of all the data on a regular basis (usually in periods of low-volume traffic). In such instances, some thought should be given as to how the on-demand scanning is scheduled.

- It is recommended to scan data prior to running backups. This ensures the data you are backing up is virus-free.

- You should examine the size and type of data you are scanning. This will affect the time taken to scan the data. Where you have large volumes of data, you may wish to break the scanning down into manageable segments -

(See "Anti-Virus" on Page 16)

Anti-Virus

(Continued from Page 15)

scan a different segment each week night while the server is less active and then scan all the data over the weekend.

How is the anti-virus software installed?

Depending on the size of the business, you may already have tools or infrastructure for deploying software to PCs (such as SMS, Tivoli). If this is the case, you may look to deploy your anti-virus software using these same software deployment tools.

However there are several areas to consider:

- It is very likely you will want to customize the setting of your anti-virus tool as part of your deployment.
- You may need to update the product with newer virus definition sets, engine components or patches. Can these be wrapped up and included in your deployment strategy as a single install?

The McAfee Installation Design utility allows you to rebuild the install MSI package and customize options such as the anti-virus components you wish to install, import the configurations of the components and apply new virus definition files, engine updates, and where required, patches as a single new install process.

Alternatively you may look to your anti-virus vendor to provide you with tools to either build a customized install package, or provide you with an enterprise management solution. Different environments require different solutions. Does your vendor provide you with a management tool to suit your requirements? Does your vendor provide consulting services to support deployment efforts?

Network Associates offer two installation and management tools – ePolicy Orchestrator (ePO) and Management Edition. Table 1 on the next page compares the current functionality between ePO 1.1 and Management Edition 2.5.

You should review the ability of any anti-virus management tools to integrate with your existing anti-virus deployment and management tools. For example, does the anti-virus management tool allow you to maintain, upgrade, and enforce policy settings for existing anti-virus tools you already have deployed, both current and older versions? Can it support autonomous installations of the product, or does it need to be pushed out with the anti-virus tools to be able to manage them?

ePolicy Orchestrator allows the management of autonomously installed anti-virus software. It supports the policy management of the following products:

- VirusScan 4.03(a)
- VirusScan 4.5
- VirusScan Thin Client (TC) 6.0
- NetShield for NT 4.03(a)
- NetShield 2000 (v4.5)
- GroupShield Domino 5.0

How are the anti-virus tools options configured and enforced?

As previously mentioned, the components such as the on-access scanner contains a host of options, including what to scan, actions to be taken on virus alert and alerting/reporting. Consideration and planning should be given to understanding these options and setting them appropriately to your threat.

Later in this document we will give some basic advice on what these settings should be.

When setting these options, you should also determine how these options and settings will be enforced. From experience, we find that users through accident or purpose will often change settings or even disable the anti-virus software installed. You must be able to monitor and control the anti-virus products you have deployed to ensure enforcement of the policies you have set, such as the specific product version as well as its configuration. In an emergency such as a virus outbreak, you should also consider how effectively you can alter or increase your scanning options.

Where using an on-demand scanner, the task should be scheduled to function automatically and have permissions to access all data, preferably from a central source. This makes management easier. Normally, we would suggest on-demand scans on servers should be run when the server in relatively inactive. If you are scanning large segments of data, your policy may include a maximum scan limit to the scan if it encroaches on other maintenance activities. In such an instance, it is important you are informed that the scan took longer than desired so you can alter the scheduled scan event.

(See "Anti-Virus" on Page 17)

Anti-Virus

(Continued from Page 16)

TABLE 1.

	ePolicy Orchestrator 1.1	**Management Edition 2.5**
Installs Anti-Virus Components	Yes	Optimized for Installs, multiple repositories
Management tool must install Anti-Virus components to be able to manage them	No	Yes
Methods of installing management client to PC	Push, e-mail, scripted, manual	Push, manual, scripted
Policy Management	Real-time enforcement	When initiated at console
Virus Reporting	Drill-down graphical reports	Tabular Virus logging
Coverage Reporting	Drill-down graphical reports	Summary text reports
Networking protocol support	HTTP/IP	IP, IPX, NETBEUI
Maximum numbers of clients manageable from single console	100,000	5000
Support for linked management consoles	Yes, merge reporting only	Yes

When deciding where to create scan tasks using the on-demand scanner, some thought should be given to the outbreak scenario. In these instances, you may wish to run on-demand scans against all machines. This can be from a scanner stored on a central server or from the local machine. In either instance, the important aspects to consider are being able to trigger the scan immediately, ensuring all files on one machine are scanned, and results are audited, and users can not disable the scan task. As the scan on large drives can take some time, this is a common tendency amongst end users.

Auditing your strategy

Once the anti-virus software has been deployed, you will want to maintain it and also be able to audit the effectiveness of your strategy.

1. Product coverage. The anti-virus tools you think you have deployed are actually out there, functioning correctly and being updated according to defined intervals.

2. Virus reporting. You can track the virus alerts and if set their removal. This is important not only to prove your anti-virus strategy is effective, but equally if you have auto-disinfection set for viruses with the OAS. You need to log the virus alert so if there was an associated payload for the virus you can be aware of it and take appropriate actions. More information on this will be covered in the section on virus outbreak procedures.

McAfee's ePolicy Orchestrator offers a level of reporting unsurpassed in the industry. Through the collation of information reported back to ePO from the client agents, ePO uses SQL queries and Crystal 7 report templates to create tabular and graphical drill-down reporting on the level of users being managed, the anti-virus components installed (by product, Engine and Virus Definition/DAT files), the effectiveness of the anti-virus software installed and the viruses detected.

ePO includes a number of different templates that allow reports to be created from a number of views, such as for a particular virus alert; for a specific infected user, the types of viruses, or the products which detected the viruses.

ePo offers coverage reporting for the following products:

- VirusScan 4.03(a)
- VirusScan 4.5
- VirusScan Thin Client (TC) 6.0
- NetShield for NT 4.03(a)
- NetShield 2000 (v4.5)
- GroupShield Domino 5.0

In addition, ePO has virus-alert reporting for the following products:

- VirusScan 4.5
- NetShield 2000 (v4.5)

(See "Anti-Virus" on Page 18)

Anti-Virus

(Continued from Page 17)

- GroupShield Exchange 4.5
- GroupShield Domino 5.0
- WebShield SMTP 4.5

Our advice for OAS policy settings

The following are some guidelines for configuration settings that should be used within your on-access scanner (OAS).

Don't scan everything. Traditionally, anti-virus is not the primary skill of most IT staff. As such, the array of options can be, to say the least, overwhelming and confusing. So what should you scan for?

• Scan only vulnerable data - Many file formats and even some operating systems do not support viruses. To scan these does not add any value to your anti-virus strategy. Look to your anti-virus vendor for advice, or even an automated method or ensuring your physical policy settings are only checking vulnerable data.

• Scan only what is local to the machine - We provide anti-virus tools for the different levels of threat from workstation (VirusScan) through server (NetShield), mail (GroupShield) and gateway (WebShield). At each point you ascertained a threat during your risk assessment, implement an anti-virus tool. This should only scan that local threat. Scanning remote data is both unnecessary and an expensive use of network bandwidth.

• Decide whether to clean - The on-access scanner's ability to remove non-memory- resident viruses on detection is an invaluable feature to the administrator. However, it is important that we have an effective method of auditing what and where the alert was. This allows the organization to prove the effectiveness of the anti-virus strategy. It also allows the IT staff to understand any further actions they may have to take against the virus infection, such as restoring data that was corrupted by the virus payload.

• Enforce the policy - User permissions can be set to prevent them tampering with the anti-virus software. When a user has succeeded in changing the settings, either notify administrators or re-enforce the policy set upon the user.

Updates Policy

Anti-virus software is only as good as its last update. Commonly one or two of the viruses we see in the top ten list is a new virus. However with weekly virus definition updates, and customers starting to request daily updates, McAfee is starting to see anti-virus security taking over from the main function of the business.

When reviewing the update policy, it is important to balance the virus risk against the frequency and ease of updating. Traditionally bandwidth has been an issue, but with automated technologies allowing both network and web updating, you should be able to apply updates with little effort. Today McAfee uses incremental updates at approximately 100KBytes per week – bandwidth concerns are no longer an issue with our products.

It is important to note that an update policy should look at all levels of updating. Within McAfee products, we offer three levels of update.

• **Virus definition update (DAT)** - The weekly incremental updates that define what viruses we can detect.

• **Scan Engine upgrades (SuperDAT)** - McAfee generally updates the scanning engine on a quarterly basis. The engine determines where we scan for viruses and what actions are taken to remove the virus code. We have found many organisations focus on the DAT updates but miss engine updates. This can result in the anti-virus software being aware of the latest viruses, but in some instances not being able to detect them (as we can not scan in the right places to detect or clean the virus).

• **Emergency Virus definition updates (incremental or extra DAT)** – These are used as an instant detection and repair solution for a new virus sample, to give you protection against current virus threats until we add the solution to the main virus definition set. The McAfee AVERTLabs website classifies new viruses according to the level of threat. If the McAfee AVERT (Anti-Virus Emergency Response Team) organization rates the virus as a medium or high priority, McAfee will produce a new incremental virus definition set. This can be applied using the normal procedures you have set in your strategy. For all new viruses, we also produce an extra DAT file, which is a simple text file that when added to the working directory of the anti-virus scanner is loaded on next startup of the OAS or as you run an ODS. Some consideration should be given to the application of the extra DAT file within your anti-virus strategy. They are

(See "Anti-Virus" on Page 19)

Anti-Virus

(Continued from Page 18)

normally applied to deal with a outbreak of a new virus. As such, you should have a fast method of implementation, that may expedite normal procedures. You should also consider prioritizing its distribution using the concepts outlined below.

So what should you consider when reviewing your update policy?

Primarily you should consider when and how you achieve your updates. We would suggest incremental update as the best method, because of its size and simplicity. The update technology with the product allows updates to be applied without either specific user permissions or reboot. In terms of frequency, you should return to your virus risk assessment for your business, and prioritize the threat. If we return to some of the examples used earlier, we can set risk levels associated with virus infection to each data point.

• Data Servers - High - These contain the core data of the business.

• E-Mail Servers - High - Most common point of virus transfer.

• Internet Gateways - High - Common point of virus entry to the organization.

• Laptops - High - Often have remote access to the business, but can gain access to media outside of the organization.

• Networked PCs - Medium - Point at which most viruses trigger and replicate. Often the first point of contact to physical media.

• Stand-alone PCs - Low - Virus cannot replicate easily.

• UNIX Machines, Backups, Document Management Systems - Low - Can be used to store virus only.

In the perfect world, we would update each of these with daily or weekly updates. However where this is not possible, you should look to maintain the level of update balanced against the threat.

This approach is also very useful when dealing with a virus outbreak. By highlighting the key threat areas, you can ensure the critical systems are updated with new definitions or if required a new engine, as soon as they are available. All other points should be updated as soon as possible but this procedure allows you to maximize control and limit the effectiveness of the outbreak.

Outbreak Procedures

The following are some simple guidelines as to the procedures you should follow when dealing with a virus outbreak.

1. Locate the virus in the environment and find out what the virus is called.

2. Ascertain the threat.

3. Get information on the virus from www.avertlabs.com.

4. Take appropriate actions to control the outbreak.

5. Estimate the scale of infection, allocate the required resources, and clean the virus.

6. Validate data integrity.

7. Contact any other business (units).

The steps above will help you deal with any virus outbreak. Most important is to understand the infection mechanism of the virus and any possible payload. This will allow you to take appropriate actions when dealing with the virus.

See the following examples.

Example 1
Form virus - This boot-sector virus relies on floppy disks to replicate. The payload of the virus makes the keyboard click on the 18th of each month, if using DOS and no keyboard device drivers.

Actions - This virus has no malicious payload and can only transfer via floppy. Request all users stop using floppies. Estimate how many machines are infected. Check all floppy disks in the organization, and clean any infected PCs. The impact to users is minimal. This author has seen companies shut down their networks for viruses like Form, which is completely inappropriate.

Example 2
Explore.Zip.Pak.Worm - This uses MAPI mail to replicate itself to users by auto-replying to unopened mail in the infected user's inbox and any new mail received. The payload of this virus is to truncate specified commonly used files such as .DOC and .XLS and.PPT on infection

(See "Anti-Virus" on Page 20)

Anti-Virus

(Continued from Page 19)

and then every 30 minutes.

Actions - This virus has two immediate threats - it can replicate fast and it has a damaging payload.

As an initial step to prevent the possible overload of the mail servers and control the outbreak, you should stop the mail servers. If it is MAPI-based, then restart it with administrator-only access. Although this causes incoming mail to queue, it stops the virus from being able to spread. You may also wish to sever your SMTP gateway if you believe there is a high threat of sending the virus out to customers. Next, you should shut down any machines you believe to be infected. You do not want the payload to trigger. This will limit the spread and damage of the virus. Finally, you would estimate the scale of the infection, and then start the clean-up process.

With any virus outbreak, if you believe you have infected another business unit or company, it is a good practice to inform them. Tell them about the virus and methods for dealing with it. Most would prefer to deal with an infection at a small scale rather than suffer a large outbreak, which could possibly be traced back to your company or business unit.

Outbreak Manager

When examining how you may better control the outbreak of new mass-mailer viruses, not initially detected by your anti-virus software such was the case when the above example first hit, you should consider using one of the current tools offered with GroupShield Exchange 4.5, GroupShield Domino 5 and WebShield SMTP 4.5, which is Outbreak Manager. This scanning tool monitors the e-mail activity, looking for virus-like events. If these events are discovered, pre-defined actions can be taken to control the outbreak. For example, when dealing with a mass-mailer outbreak, we could look for a defined number of duplicate attachments. When this threshold is reached, the actions can either be manually or automatically triggered. These could include:

• Updating the virus definitions (new definitions may be able to exactly identify and clean the virus).

• Run a scan against all mailboxes or folders to clean the infection.

• Block all attachments, thus stopping the virus from replicating.

• Shutdown and restart the server with administrator-only permissions. This would allow mail to be received but would stop any users being able to open or run the infected attachments.

Outbreak Manager will not detect the virus by name. However, it will act as an early warning system. With its ability to set rules against virus-like actions, it can ensure the outbreak of a new unknown virus is limited by the actions set, so reducing the scale of the outbreak, and where defined, take the first steps towards the clean up.

Training and awareness

Obviously your everyday user is not a virus expert. However some simple employee guidelines, either in a user manual or as part of basic training will help them. The sort of information you should pass onto users is as follows:

• Basics - What is a virus? What can viruses do? How can they affect me?

• Basics - Advice on using PCs at work to avoid virus infection.

• Don’t open or run untrusted e-mails or programs.

• Get any incoming physical media checked for viruses before using it.

• Be aware of the risks of downloading games, utilities, and so on from the Web.

• Basics - Where or who do I go to for further information or advice?

• Question - How can users confirm they have anti-virus software installed?

Answer - Check for the icon in the system tray.

• Question - If possible, how do they check the are running a current version?

Answer - The Help About box includes the date of the drivers being used.

• Question - What should a user do if they see a virus alert?

Answer - Record the virus name, contact the appropriate member of IT support. If good auditing is in place, this will have been logged automatically for the user.

(See “Anti-Virus” on Page 21)

Anti-Virus

(Continued from Page 20)

Documentation

Once you have completed creating your anti-virus strategy, you should document it. This allows any member of the IT staff to understand the policies and procedures in your anti-virus strategy, and importantly to be able to complete them in your absence. This is specially crucial during a virus outbreak where a clearly defined policy can save both time and money by dealing with the virus effectively.

It is also necessary to review your virus strategy on a regular basis (at least annually). This is to take into consideration the changes within your IT infrastructure (in other words, it will re-assess the virus risk to your business) and the changes within the virus industry, such as new types of viruses, which again may require you to review and amend your strategy.

Summary

This document has provided useful guides and steps to follow when looking to create or review you anti-virus policies and procedures. If you require further help creating an anti-virus strategy, contact McAfee Professional Services or your local McAfee Sales representative.

As a final check list, you should look to complete the following sections each time you review your strategy.

1. Review your environment.

2. Set your anti-virus policies and procedures.

3. Define your update strategy.

4. Be able to audit the implementation and effectiveness of your strategy.

5. Prepare an outbreak procedure.

6. Document your strategy.

7. Make your users aware of virus threats.

Jed McNeil is State & Local Government & Education Sales Manager for Network Associates, Northern California. He can be reached at 1-800-338-8754 x3101 or by email at jed_mcneil@nai.com. Lisa Milburn is State & Local Government & Education Sales Manager for Network Associates, Southern California. She can be reached at 1-800-338-8754 x3138 or by email at lisa_milburn@nai.com.

Theme

(Continued from Page 1)

source, from anywhere will position its students to better compete in the dynamic knowledge economy. A collaborative, bolstered by the participation of many industries, has been created, to encourage the development of digital resources for a K-16 establishment.

A real time digital discourse is now evolving and the emergent applications will revolutionize the educational environment. Students will experience tele-science, tele-agriculture, virtual interactivity, realistic virtual objects and presence, and tele-immersion in remote locations. Wrap these concepts around any curriculum, perhaps History, and you can imagine the profound difference these engaging applications will make to educators, parents and students. The impact will be no less apparent on the institutions that support classrooms. Financial and human resource functions will bear little semblance to today’s operations.

These innovations are dependent upon an infrastructure that can handle converged information. This information must all be afforded a Quality of Service that today is given only to digital voice transactions. Fiberoptic transmission capacity is at the core. Support personnel who are trained in sophisticated and multifaceted analysis and problem resolution are essential to implementation, moreover must also be service oriented and handle larger work loads more efficiently. Our mission this year will be to organize information about the Digital Future in presentations on our WEB pages, in the *DataBus* and at the conference. We intend to provide assistance to our members to meet the challenges confronting them. We will illustrate the equipment that is available, the experts who can contribute and the systems that are emerging. The dialogue around this exciting digital future will be the primary focus of CEDPA’s efforts in coming months and in Monterey.

Warren Williams, CEDPA President, is Assistant Superintendent of Information and Technology Services for the Grossmont Union High School District.

Ten Steps to Exchange 2000 Server: Migrating the Othello, Washington, School District Way

Tuan Nguyen, Microsoft Corporation

So, your school, district or campus has decided to migrate from Microsoft® Exchange Server 5.5 to Exchange 2000 Server. Now, how will you do it?

Microsoft provides extensive documentation to help you make the move from Exchange Server 5.5 to Exchange 2000 Server, including the Microsoft Exchange 2000 Deployment Guide at http://www.microsoft.com/exchange/ and the Microsoft Exchange 2000 Server Upgrade Series at http://www.microsoft.com/technet/exchange/guide/default.asp. These resources detail the steps, tools and considerations you need to know as you plan and implement your migration.

But few migrations follow the "textbook" line by line. Each environment is different. Goals are different. User needs are different. And so deployments, inevitably, are different. To give you greater insight into the migration process, this document follows the actual step-by-step migration process adopted by the Othello, Washington School District in migrating to Exchange 2000 Server last year. The Othello experience can give you insights and inspiration for the customized process of your own deployment.

Background on Othello

The Othello School District in eastern Washington state is typical of many school districts around the country. It is small (population: 5,000), rural, with five schools, two maintenance facilities and an administrative center. Last year, its two-person technology staff was strapped managing the fiber-optic network with nearly 1,000 PCs and seven servers, funded by the federal E-rate program and by the community's 1997 passage of a $3.9 million dollar technology bond levy. As if that wasn't enough, each classroom would be upgraded to support four PCs and eventually include 14 labs. With maintenance issues already taking at least two hours a day, Network specialist Russ Beard knew that a major change was needed to make the management challenge practical.

For Beard and the Othello School District, that change was an upgrade from Windows NT® 4.0 and Exchange Server 5.5 to Windows® 2000 Server and Exchange 2000 Server. The software promised to enable greater centralized management, security, and simplified use, leading to higher productivity and lower total cost of ownership for the district.

"When we were in the planning stages of our migration to Windows 2000, we had discussions with Microsoft about continuing to run Exchange Server 5.5 versus Exchange 2000 Server," recalls Beard. "Compared to Exchange 5.5, Exchange 2000 promised seamless integration with Windows 2000 Active Directory™ service, which is what I was personally looking for to help reduce the management burden. It would be easy to extend the schema to the global catalog and to run Exchange from the snap-in in the management console. This easy use was crucial to freeing up scant staff resources."

Prolog: Testing and Planning for Exchange 2000

But would the reality meet the promise? In spring 2000, Beard took a close look at Exchange Server Release Candidate 1 and built his own test server using RC2.

"I was impressed with the results," says Beard. "The installation in the test lab was very smooth and I was impressed with how easy it was to run and to integrate the Release Candidate into Active Directory. However, I've never found that a test lab experience pans out exactly the same in real life. I did a larger mock environment in which I put everything on a single server, to test DNS, how the global catalog would transmit across multiple servers, and so on. I did the installation twice, reformatted and did it again, then attached a couple of clients."

With this actual hands-on experience with RC2, Beard was comfortable making Exchange 2000 Server a part of his broader migration plan. As a conservative approach to minimize the potential for problems, he decided not to migrate Windows Server 2000 and Exchange 2000 Server at once. Rather, he would complete the operating system upgrade and then, when he was confident that it was operating successfully, he would move the district onto the Exchange Server upgrade as a second step.

Beard continued his testing of Exchange 2000 Server into summer 2000. He put together a plan and budget for the district administration, one that would restructure the network in an important way. Previously, the server for

(See "Exchange 2000" on Page 23)

Exchange 2000

(Continued from Page 22)

each school hosted all functions for that school – file storage, applications, data, and so on. To take maximum advantage of Windows 2000 in general and Exchange 2000 Server in particular, Beard would bring the servers offline – maintaining a skeletal, two-server Windows NT network in the interim – and restore each in a Windows 2000 domain as a single-function server, including one server dedicated to Exchange 2000 Server, thereby optimizing bandwidth and performance on the network.

One key consideration for Beard was whether or not to preserve the existing mail messages, calendars, address books, and other data of his users contained in the Exchange Server 5.5 information store. Although the "move mailbox" migration method outlines a way to permit this, Beard decided on a clean, out-of-the-box installation of Exchange 2000 Server coupled with specific instructions to his users to enable them to backup and restore important personal information such as addresses and calendars. Beard regarded this as an expedient choice given his limited time and resources.

Beard completed the Windows 2000 migration during summer 2000 (see *Othello, Washington School District Migrates to Windows 2000 To Gain Benefits of Manageability, Security* on the TechNet for Education web site at http://www.microsoft.com/technet/education/othelfin.asp). As a last step before students and teachers returned in the fall, he completed the Exchange 2000 Server upgrade as well.

Step 1: Backing Up Mailboxes

The migration to Windows 2000 and, subsequently, Exchange 2000 Server, would take place over the summer. However, the first step in the migration to Exchange 2000 Server actually preceded this. To ensure that all users would retain the address book and calendar information in their Outlook® messaging and collaboration client files, Beard gave them instructions on how to preserve this information in June, before many employees left for the summer.

To make this step simple for users, Beard directed them to the "Export to PST File" Wizard in Outlook. Its import/export command allows users to specify the location for backup and provides a local hard drive location as the default. This was ideal for the Othello migration, since users were generally retaining their existing desktop PCs. Beard also directed users to name the file with their own name and the .PST extension – such as Russ.pst. By clicking on the top of the Outlook tree displayed in the Wizard, users could choose to "include all subfolders" to maintain their full personal contact and calendar data. To streamline the process, Beard also encouraged users to first empty their deleted and sent mail items and to clean out unneeded messages and files prior to the backup.

"I've seen users backing up 40MBs of data or more," says Beard. "With all users doing this at the same time, it can affect network bandwidth. Encouraging users to delete unnecessary files first can help mitigate this concern."

Step Two: Work from a Successful Deployment of Windows 2000 Server

After completing his migration to Windows 2000 – including creation of a new, single-domain forest – Beard was ready to begin the migration to Exchange 2000 Server. He was now running a stable Windows 2000 network in native mode.

Earlier, he had upgraded his server hardware from Intel Pentium IIs to AMD/Athlon processors and from an average of 250 MB RAM to full 1GB RAM. The upgrades cost an average of $2,500 per machine – which Beard considers a "bare bones budget" price for the school district, making the upgrade to Windows 2000 and Exchange 2000 Server both feasible and worthwhile. It was one of these upgraded boxes that Beard used for the Exchange migration.

Beard prepared his proposed mail server by loading it with Windows 2000 Advanced Server SP1. He joined it to the existing Windows 2000 domain by right clicking on My Computer, selecting properties, and then choosing the Network ID tab. On the face of this applet he clicked the button properties, and made sure to have the proper computer name in the appropriate space. In the box for domain, he entered the name of the new domain. Then he entered a user name and password with Administrative privileges. The system welcomed him to the new domain and he rebooted the computer. At this point, the server needed no further configuration.

Step Three: Prepare the Domain Controller

Beard turned his attention back to his existing Windows 2000 domain controller, confirming that both DNS

(See "Exchange 2000" on Page 24)

Exchange 2000

(Continued from Page 23)

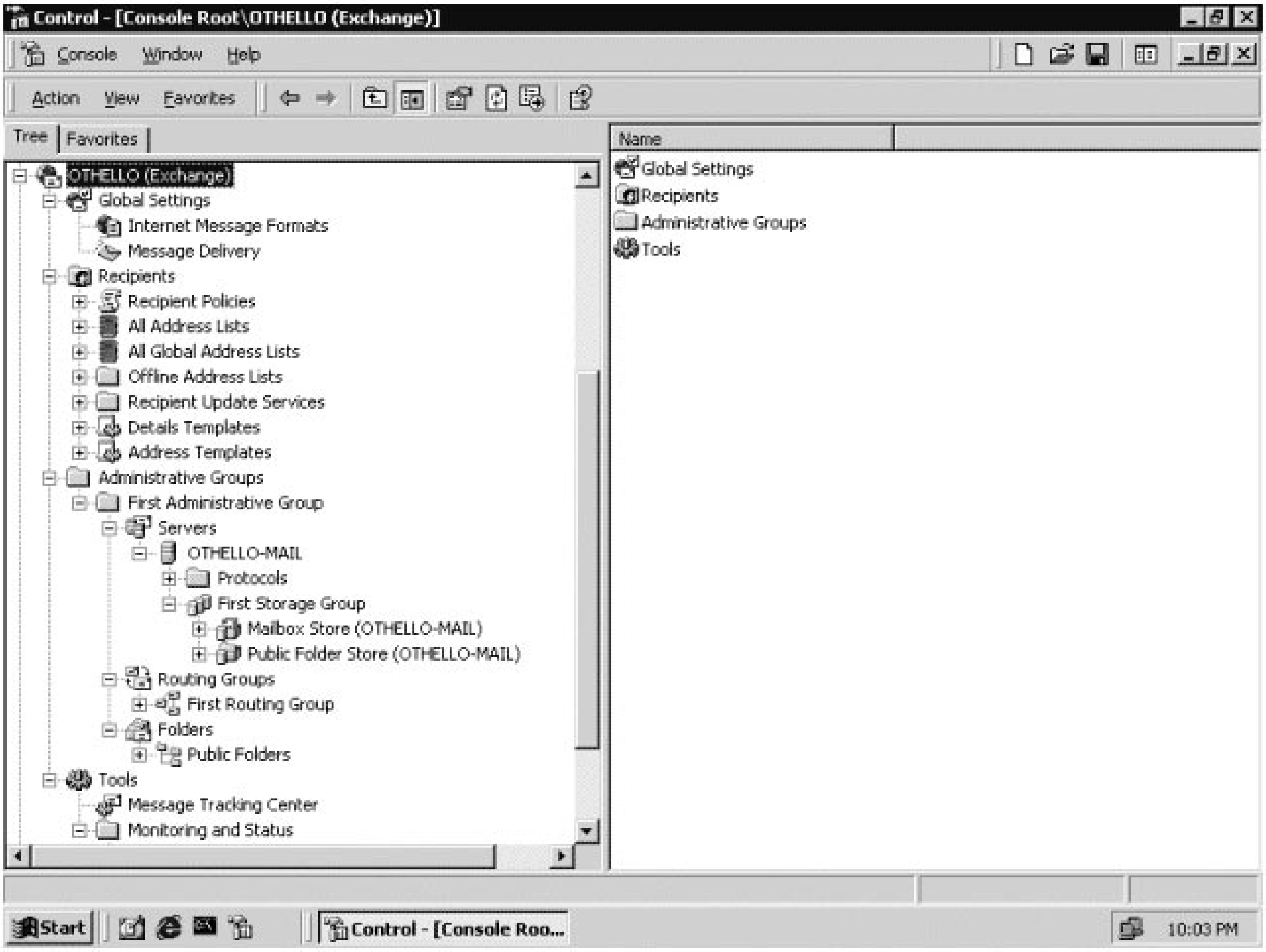
and DHCP were configured and running. To do so, he found it helpful to build a control console. He went to Start/Run, entered “mmc” and hit enter. The Microsoft Management Console opened and he built a console by going to Console and clicking Add/Remove Snap-ins. He clicked the Add button and selected the snap-ins that he needed. With the console built, he saved it to a convenient location. From the console he had two ways to check the DNS and DHCP servers: simply looking at their activity or by going to the Services Module. Some districts may be like those in Othello’s Washington state, which generally don’t do their own DNS work and rely on the state network for this service. If so, now is the time to begin to manage DNS locally, according to Beard.

The Othello School District management console in Windows 2000

“Windows 2000 relies on DNS for so many things so it’s critical to set it up right,” says Beard. “DNS is also extremely critical in how Exchange 2000 works because it handles all the name translation. For example, DNS is what identifies to the world that this server works for Othello. It gives an IP number to the domain name, Othello.wednet.edu. DNS has a mystique but it isn’t rocket science.”

Beard then began populating his user accounts on the Windows 2000 server, a procedure he says is not mandatory, but which he recommends because it then makes it easier to set up the new mailboxes once Exchange 2000 is loaded and extended into the Windows 2000 schema. To do so, he used a third-party “Add Users” Utility from the Windows 2000 Resource Kit, which brought the user accounts in from Windows NT to Windows 2000 in a CSV file. This tool is the same one that can be used in migrating accounts within a Windows NT 4.0 network.

(See “Exchange 2000” on Page 25)



Exchange 2000

(Continued from Page 24)

Beard points out that the User Migration Wizard is also an ideal way to accomplish the migration of users from an old Windows NT domain to a new Windows 2000 domain and that this Wizard has worked well for him also. The caveat is that the domain must already be functioning in native mode to use the Wizard, which doesn't function in mixed mode networks.

A crucial, final aspect of preparing the domain controller was to make sure that Internet Information Services built into Windows 2000 (IIS) was set up and running on at least one machine in the domain. To do this, he added the IIS snap-in to the control console and then double-clicked the IIS tree. This was important, says Beard, because SMTP – a necessary mail protocol – wouldn't work without IIS being active. Beard also confirmed that another necessary service, the remote procedure service (RPS), was installed and running.

"Exchange 2000 Server requires a number of services to be up and running on the domain, such as DNS, Active Directory, RDS, RPS, IIS," says Beard. "But the neat thing about the installation of Exchange 2000 Server is that you can't make a mistake. As Exchange installs on the server, it will look for these services and, if they're not there, active and configured, Exchange will stop the install process and tell you that it can't continue for this reason. I have to say that this aspect of the installation works very well."

Step Four: Using ForestPrep to Extend the Schema

The Windows 2000 Active Directory service schema must be extended to support the diverse attributes in a messaging application directory. Exchange 2000 extends Active Directory with new Exchange attributes, allowing users, groups and contact objects in Active Directory to become mail recipients. Existing Active Directory attributes are also modified, some of which affect what Outlook users see in the global address list. The schema is extended only once. Beard chose to extend the Othello schema by using the ForestPrep utility located on the Exchange Server CD-ROM. ForestPrep prepares the Windows 2000 forest for Exchange. It prompts for and creates the Exchange organization name and object in Active Directory, building the initial Exchange organization structure. When Exchange is then installed, Setup can then query Active Directory for configuration information. ForestPrep also assigns Exchange full administrator permissions for the specified administrator account.

ForestPrep was separated from Exchange 2000 Setup because Setup must perform operations that require permissions of an Enterprise Administrator and Schema Administrator and – although this wasn't an issue for the relatively small Othello – much larger enterprises may not be comfortable providing this level of permissions to Exchange administrators. In other words, the set of permissions required for Exchange installation are of a higher level than the set required in production. So, in enterprises with larger staffs and greater divisions of responsibility, ForestPrep is run by the Windows 2000 Enterprise Administrator as a separate, preliminary setup function.

In Beard's case, because he had responsibility both for deploying Exchange and also for modifying Active Directory schema, and because he had only one Windows 2000 domain, he could have chosen to run ForestPrep (and DomainPrep) as part of Exchange Setup. In fact, when he ran ForestPrep separately, a dialog box told him that, because he had only one forest and one domain, he did not need to run the utility. Nevertheless, Beard chose to run it and says he found it part of a "flawless" installation.

"I found it a good procedure to extend the schema this way prior to loading Exchange," says Beard. "It helped ensure that there were no hiccups in loading files later on in the process. It may not be necessary but it won't hurt anything and I believe it made my installation go smoother."

Step Five: Using DomainPrep

Beard next ran DomainPrep on the server.

DomanPrep is analogous to ForestPrep (see Step Four) and prepares the domain for Exchange 2000 Server much as ForestPrep prepares the forest for the new email software. DomainPrep creates two security groups in each Windows 2000 domain in which it is run. Together, the groups provide permissions to Exchange servers, so that the servers can perform tasks such as modifying Exchange user attributes. A Windows 2000 domain administrator must run DomainPrep in any domain where Universal Security Groups (USGs) will be installed, where mail-enabled users will reside, or where, as in this case, an Exchange Server will be installed.

DomainPrep creates and configures permission for the groups in the following table:

(See "Exchange 2000" on Page 26)

Exchange 2000

(Continued from Page 25)

Group	Function	How populated	Permissions
Exchange Domain Server	A global security group that lists the machine accounts of all servers running Exchange 2000 in each domain.	It's populated by Exchange setup when you install a server.	It has read-only permissions to the Exchange System Manager.
All Exchange Servers	A domain local security group that contains all Exchange Domain Servers groups from all domains, used for granting access.	The RUS adds the Exchange Domain Servers groups from all other domains that have an active RUS.	It has Modify permissions on all Active Directory recipient objects.

In addition, Beard specified the Address List Server using DomainPrep. Since Exchange 2000, unlike Exchange Server 5.5, no longer has a directory of its own but uses Active Directory, address book lookups have changed. One ramification of this is the requirement to choose an address list server.

Because Beard was setting up a relatively small forest with a single domain, catalog replication was a concise process; for big forests with multiple domains, catalog replication could be time consuming, he warns.

Step Six: Install Exchange 2000 Server

With the server box now fully prepared and configured with Windows 2000, Beard was ready to install Exchange 2000 Server on it. The process of loading Exchange 2000 Server from the CD-ROM took about an hour for the complete installation that Beard used. Because Beard had used DomainPrep and ForestPrep, the work of loading and configuring the Exchange server itself was relatively straightforward.

"Installing Exchange 2000 Server isn't the same as installing Exchange Server 5.5," says Beard. "With 5.5 you're setting up the server to work with different domains, domain controllers, primary domain controller, and so on. With Exchange 2000 and Windows 2000, it's all one entity. One machine in the forest is the global catalog, where the schema resides and where Active Directory functions take place, regardless of whatever else you're running."

Installing Exchange 2000 Server on a new server, rather than directly upgrading the existing Exchange 5.5 server, had a key benefit for Beard and Othello. Beard could test and confirm the operation of the new server without affecting the older mail server or the users continuing to rely on it during the migration.

Step Seven: Reboot and Confirm DNS Pointing to Exchange

After installing Exchange 2000 Server, Beard rebooted both systems – the Exchange 2000 Server and the Windows 2000 domain controller – to confirm their proper operation.

"Microsoft talks about minimizing or eliminating the need to reboot and I don't know that their documentation recommends a reboot at this point, but I'm conservative about these things and it seemed like the right thing to do," says Beard.

Certainly, rebooting gave Beard a chance to see his two new servers come up together properly, giving him added confidence to continue with the installation procedure. His next step was to ensure that there was a DNS MX entry for the new Exchange 2000 Server. The MX (mail exchange unit) entry is the identification in the DNS table that directs mail entering the domain to the domain's mail server. The entry needed to be updated to reflect the Exchange 2000 Server, so that incoming mail could be processed by Exchange 2000 and reach its intended recipients.

To confirm the MX entry update, Beard went to the domain controller's management console, and chose the DNS level from the directory tree. This contains the root DNS records including the MX entry. Beard confirmed that the entry was pointing to the new domain and to the new Exchange 2000 Server.

Step Eight: Install Exchange System Management Tools

Beard now had his Exchange 2000 Server up and running with the DNS aware of the new server and prepared to point incoming mail to it. His next step was to install System Manager, the Exchange system management tools, into the domain controller management console. With System Manager, he would be able to manage

(See "Exchange 2000" on Page 27)

Exchange 2000

(Continued from Page 26)

the new server fully and effectively from a central location, just as if he were sitting in front of the server. He also chose to install Terminal Services so he could run the management tools remotely from any location – in the field, at one of the schools, or even from his home.

To install the management tools, Beard chose Auto Run from the Exchange Server CD-ROM. Instead of choosing Typical Install, he changed the default to Install System Manager, responded to a few additional screens, and installed the software.

“With one console, Windows and Exchange allow me access to every management tool, so I can easily manage my entire server array,” says Beard. “I even installed Terminal Services on my laptop. I dial-up from my laptop when I’m at home and I can administer the Exchange server from there. I’m using a basic 42K dialup connection and it works fine. I can’t say enough about what Microsoft has done with these tools and Terminal Services.”

Step Nine: Confirm Settings in the Exchange 2000 Server System Manager

With the Exchange System Manager installed, Beard next reviewed its settings to ensure that they were configured properly for the needs of the Othello domain. For example, System Manager enabled him to put limits on mailboxes, to reclaim deleted items from Outlook and to create tombstones. System Manager also enabled Beard to access the Information Store and Public Folders.

Beard confirmed and configured the System Manager settings by moving through the series of nodes in the directory tree (see Console diagram, above).

- The first node, Global Settings, contains Internet message formats and Message delivery containers. It gave Beard the option to filter incoming mail.
- The Recipients container node covers recipient policy, address book views, update services, and several templates. It supports separate address book views and policies for specific users.
- The Administrative Group node is the heart of Exchange Server. Each server or groups of servers can be assigned administrative groups, for organizing recipients or balancing resources. A Servers node holds the container of each specific server. Under the server is the protocols folder as well as the Storage Groups. Inside Protocols are the specifications of all the protocol settings for the Exchange site. The Storage Group contains both the private information store and the public folder store. It allows the administrator to divide an organization into separate storage groups to impose separate policies and to provide enhanced security. This group also contains the Routing group folder and the folder listing all public folders created on the site.
- The Tools node supports the Message Tracking Center, for tracking the use and efficiency of the Exchange site. It also supports the monitoring and status folder, which Beard used to build monitors to alert him to Exchange server problems.
- The node for Active Directory, Users and Computers enables the addition or deletion of users to the site.

Step Ten: Restoring Client Data and Creating New Profiles

Now, Beard was ready to guide his end users through the process of removing their old, Exchange 5.5 server-based profiles from Outlook, to create new profiles for Exchange 2000 Server, and to restore the personal address book and calendar information that they backed up to their local hard drives at the start of the process.

To do this, Beard directed users to the Properties section of Outlook to delete the existing Profile. Users were then directed to Add New Profile, and to choose the Exchange 2000 Server for that Profile where the screen asked them for the new server name. Using Outlook, they also chose Import PST File to bring back their previously saved personal address and calendar information.

With the user profiles restored, users could now communicate with the new server, sending and receiving email, files, calendar data and other information. From the user perspective, the migration was complete and successful.

Beard was now able to take the old Exchange 5.5 Server and remaining Windows NT 4.0 domain controller off the skeletal, interim domain. Those machines were then refurbished and brought back into the new domain as Windows 2000 servers, completing the migration.

Tuan Nguyen is K-12 Education Marketing Manager for Microsoft Corporation’s Southern California District. He may be reached by telephone at (310) 449-7408 or by e-mail at tuanng@microsoft.com

President

(Continued from Page 3)

least, by having access to many bid proposals and other information as it relates to bids, our members can assure their organizations of well prepared documents. Bid Central could also list bids that are current from around the State including information on CMAS, Calnet and other statewide instrument for purchasing equipment or services.

As you can see, our goals are ambitious but attainable. I have also not detailed an exclusive list of services that we might offer. The Board of Directors is committed to bringing you any help to assist you at work. We would appreciate any input you might give before the development of these services to make sure we include features that you would like to see. We will also design in a feedback mechanism so that you might give us additional input once the service is available.

CEDPA
P.O. Box 6552
Huntington Beach, CA 92615-6552