BIBLIOTEKA INFOTELA

Cena 15 zł (w tym 0% VAT)
ISBN 83-921962-1-X

SIECI LOKALNE I KORPORACYJNE

I SPARTAKIADA Branży Komunikacji Elektronicznej

SŁOK k/Bełchatowa, 22–25 sierpnia 2005

organizator: ul. Stawowa 110, 85-323 Bydgoszcz
tel. (52) 325 83 16, fax (52) 373 52 43
tel. kom. 607 152 817
e-mail: arek@msgmedia.pl
www.techbox.pl

MSG MEDIA

zapraszamy do uczestnictwa

www.zpas.pl
www.zpas.net

Obudowy teleinformatyczne

Obudowy energetyczne

Szafy zewnętrzne dostępowe

Okablowanie strukturalne
i osprzęt telekomunikacyjny

Pulpity dyspozytorskie i sterownicze
oraz synoptyczne tablice mozaikowe

System nadzoru
ZPAS Control Oversee

Najlepszy polski wyrób
na targach Intertelecom 2005

ZPAS S.A.

Telefon: 074 / 872 0 100 (centrala)
Faks: 074 / 872 40 74, 872 55 92
e-mail: info@zpas.pl;
Internet: http://www.zpas.pl

ZPAS-NET

Telefon: 074 / 872 0 122 (sekretariat)
Faks: 074 / 872 58 56
e-mail: info@zpas.net;
Internet: http://www.zpas.net

Grupa ZPAS

Drodzy Czytelnicy, niezwykle miło mi zaprezentować firmy ZPAS SA i ZPAS-NET w ramach Biblioteki Infotela. Mamy ponadtrzydziestoletnią historię i z powodzeniem przeszliśmy okres transformacji (w tym prywatyzacji) na początku lat dziewięćdziesiątych. Ciągle rozwijamy się i realizujemy poważne inwestycje, dzięki czemu nasz zakład bardzo często przedstawiany jest nie tylko jako przykład nowoczesności, ale także jako przykład sukcesu grupy ludzi, którzy wierzą w powodzenie swoich działań i nie obawiają się realizacji trudnych zamierzeń. Niniejsza publikacja stanowi zaledwie wycinek informacji o nas, dlatego zapraszam zainteresowane osoby do odwiedzenia naszych stron (nie tylko internetowych), nie tylko dlatego, że zakład znajduje się w niezwykle malowniczym regionie Pogórza Sudeckiego, ale również, aby zapoznać się ze stosowanymi rozwiązaniami, wynikającymi z potrzeb naszych klientów.

Odnosząc się do sfery produkcji warto zaznaczyć, że ZPAS SA jest firmą oferującą dość szeroką gamę wyrobów i trudno wydzielić jedną branżę, w której zmieściłby się profil zakładu. Na ogół producenci podobni do nas skupiają się na produktach przeznaczonych tylko dla energetyki bądź tylko telekomunikacji, natomiast my te branże staraliśmy się integrować już w drugiej połowie lat 90., kiedy np. idea internetu w gniazdku sieciowym jeszcze uważana była za fantazję. Obecnie rozwijamy integrację obudów teleinformatycznych i energetycznych próbując stworzyć wspólną platformę, co z pewnością pozostaje w związku z rozwojem branży IT, która coraz bardziej wkracza we wszystkie sektory i obszary gospodarki i przemysłu. Raporty TELEINFO 500 czy Raport Computerworld w ostatniej edycji klasyfikowały nas na czwartej pozycji w kraju w tabeli producentów sprzętu telekomunikacyjnego, mogę więc przyjąć, że jest to dominujący obszar zainteresowania naszej firmy.

Piotr Baranowski
prezes zarządu ZPAS SA

ZPAS

Wyroby produkowane w Przygórzu najczęściej stanowią teletechniczne zabezpieczenie nowoczesnych systemów telekomunikacyjnych, informatycznych i energetycznych. Firma ZPAS w czerwcu 2004 roku podzieliła się na dwa zakłady: ZPAS SA i ZPAS-NET sp. z o.o.

Nowe rozwiązania technologiczne tej firmy pozwoliły stworzyć jednolitą i kompleksową ofertę produktów. Wyroby ZPAS SA i ZPAS-NET dzięki tym rozwiązaniom pozwalają na połączenie wcześniej rozdzielonych grup produktów branży informatycznej i energetycznej.

Oferta ZPAS SA obejmuje obudowy teleinformatyczne 19" i 21" (w tym szafy serwerowe, telekomunikacyjne, kompatybilne elektromagnetycznie oraz inne w wersjach stojących i wiszących), obudowy energetyczne (stojące i wiszące) oraz obudowy w wykonaniu specjalnym. Oferta ZPAS-NET zawiera elementy okablowania strukturalnego, osprzęt telekomunikacyjny, szafy zewnętrzne dostępowe, szafy i rozdzielnice z wyposażeniem elektrycznym, pulpity dyspozytorskie i sterownicze, synoptyczne tablice mozaikowe, rozproszony system nadzoru ZPAS Control Oversee.

ZPAS SA posiada certyfikat zapewnienia jakości ISO 9001:2000 i certyfikat systemu zarządzania środowiskiem ISO 14001:1996. Więcej informacji na temat firmy znajduje się na stronie internetowej **www.zpas.pl**.

ISBN 83-921962-1-X
Cena 15 zł (w tym 0% VAT)
Nakład: 7000 egz.

Wydawca:

MSG – Media s.c.
ul. Stawowa 110
85-323 Bydgoszcz
tel. (52) 325 83 10
fax (52) 373 52 43
office@msgmedia.pl
www.techbox.pl

Partnerzy wydania

Redakcja
Rafał Mikołajczak
Marek Kantowicz
Grzegorz Kantowicz
Robert Błaszczyk

DTP
Dariusz Bartkowiak
Czesław Winiecki

Marketing
Janusz Fornalik
Arkadiusz Damrath

Korekta
Ewa Winiecka

Druk
Drukarnia ABEDIK
Sp. z o.o.
85-861 Bydgoszcz
ul. Glinki 84
tel./fax (52) 370 07 10
info@abedik.pl
www.abedik.pl

SPIS TREŚCI

Warto wiedzieć

... Oferta telefonów IP Alcatela dla biznesu, która obejmowała modele Alcatel 4038 i 4068 IP Touch, została rozszerzona o dwa kolejne: Alcatel 4018 IP Touch – model podstawowy oraz Alcatel 4028 IP Touch dla użytkowników średnio zaawansowanych. Dzięki zastosowaniu otwartych standardów – VXML (voice XML), rozwiązania Alcatela oferują swobodny dostęp do szerokiej gamy dodatkowych usług telekomunikacyjnych przeznaczonych dla pracowników, które obejmują m.in. ujednolicone systemy komunikacji i wyspecjalizowane aplikacje dla biznesu. Wśród wielu przykładowych aplikacji, które mogą być uruchamiane na telefonach Alcatel IP Touch, są: osobisty asystent, usługi rutingu połączeń, zarządzanie kalendarzem spotkań i obsługą sal konferencyjnych, usługi związane z ochroną budynków oraz programy wspierające zarządzanie hotelem. Uzupełnieniem oferty telefonów stacjonarnych przeznaczonych do współpracy z tradycyjnymi sieciami telefonicznymi TDM są 3 nowe modele: Alcatel 4019 – aparat dla rynku masowego, Alcatel 4029 – reprezentujący klasę średnią oraz Alcatel 4039 dedykowany dla najbardziej wymagających użytkowników. Telefony te uzupełniają dotychczasową linię telefonów z rodziny Alcatel Reflexes, chroniąc w ten sposób wcześniejsze inwestycje w infrastrukturę telefoniczną.

... Bank Millennium, w ramach realizacji strategii rozwoju sprzedaży kredytów hipotecznych w internecie, uruchomił aplikację CRM do obsługi zgłoszeń klientów. Aplikacja wdrożona przez firmę technologiczną eo Networks wprowadza nowe standardy w obsłudze klientów on-line. Rozwiązanie łączy działania związane z obsługą klientów banku, od pierwszego kontaktu za pośrednictwem internetu. Aplikacja jest zintegrowana ze stronami internetowymi banku oraz innych portali internetowych.

... Firma Compuware Corporation poinformowała o podpisaniu ostatecznej umowy kupna prywatnej firmy Adlex mieszczącej się w Marlborough, w stanie Massachusetts. Jedyne europejskie biuro Adlex mieści się w Gdańsku. Transakcja opiewa na ok. 36 mln dolarów, a jej finalizacja ma się odbyć w najbliższym czasie. W jej wyniku ok. 80 pracowników firmy Adlex znajdzie zatrudnienie w Compuware. Firma Adlex jest pionierem technologii zarządzania dostarczaniem usług (*Service Delivery Management* – SDM), która umożliwia operatorom internetu i klientom korporacyjnym diagnozowanie aplikacji dostarczanych użytkownikom oraz zarządzanie ich jakością. Zapewniając ogromną funkcjonalność, monitorowanie komfortu pracy użytkowników bez użycia agentów oraz szczegółową analizę wydajności aplikacji, technologia ta uzupełnia linię produktów Vantage firmy Compuware.

... Crowley Data Poland, operator telekomunikacyjny, dostawca rozwiązań transmisji danych i głosu, od maja 2005 r. oferuje swoje usługi odbiorcom na rynku łódzkim. Crowley gwarantuje użytkownikom radiowy dostęp w technologii LMDS w promieniu nawet do 30 kilometrów od centrum miasta, ulicy Piotrkowskiej, przy której zainstalowano stację bazową. Klienci Crowley, poza profesjonalnym dostępem do internetu, będą mogli skorzystać m.in. z kompleksowej usługi telefonicznej TeleKontakt, umożliwiającej obniżenie kosztów prowadzonych rozmów telefonicznych nawet o 40 proc. W najbliższym czasie firma planuje także instalację w Łodzi najnowocześniejszych urządzeń zapewniających transmisję w nowym standardzie WIMAX.

... Energis Polska i Inotel podpisały umowę o współpracy. Na jej mocy operator będzie mógł dostarczać klientom profesjonalne usługi telefonii internetowej w oparciu o platformę Inotel. Energis będzie oferował usługi telefonii internetowej za pośrednictwem swojej sieci partnerów, resellerów oraz samodzielnie. Firmy, które zdecydują się na podłączenie do platformy Inotel, będą mogły telefonować za pomocą specjalnych aparatów telefonicznych (tzw. IP Phone), bramek VoIP, do których można podłączyć dowolny aparat telefoniczny, lub przy pomocy słuchawek i mikrofonu podłączonych do komputera.

... Funkwerk Enterprise Communications wprowadziła na rynek nowy telefon VoIP – elmeg IP290. Telefon posiada dwuwierszowy wyświetlacz graficzny oraz układ klawiatury dostosowany do standardów przemysłowych, co umożliwia jego intuicyjną obsługę. Pięć dowolnie programowanych przycisków pozwala na błyskawiczne odnajdywanie numerów, pod które najczęściej dzwonimy i na natychmiastowe

ustanawianie połączenia z tymi numerami. Telefon wspiera wiele funkcji znanych z sieci telefonii konwencjonalnej, takich jak „oddzwanianie gdy numer jest zajęty" czy przekierowywania połączeń. Książka adresowa pozwala zapisać do 100 numerów. Telefon posiada pamięć połączeń nieodebranych, klawisze szybkiego wybierania, funkcję zawieszania połączeń czy też przekierowywania połączeń. Elmeg IP290 został wykonany w opcji wielojęzycznej. Dodatkowy port Ethernet ze wsparciem VLAN umożliwia podłączenie telefonu IP bezpośrednio do komputera. Aparat współpracuje z oprogramowaniem Microsoft Messenger, a także ze standardowymi urządzeniami oferowanymi przez innych producentów.

... Juniper Networks podał, iż podpisał wiążące umowy przejęcia Peribit Networks, lidera w technologii optymalizacji sieci WAN, oraz Redline Networks, pioniera w rozwoju technologii Application Front End (AFE). Transakcja przejęcia Peribit Networks wyceniana jest na około 337 milionów dolarów w gotówce, akcjach i opcjach na wykup akcji. Transakcja przejęcia Redline Networks wyceniana jest na około 132 milionów dolarów w gotówce i opcjach na wykup akcji.

... W maju br. firma MCX Systems wprowadziła na rynek nową linię rozwiązań telekomunikacyjnych NeXspan. Są to serwery teleinformatyczne nowej generacji, integrujące tradycyjne systemy łączności z technologiami IP. Na linię NeXspan składają się cztery modele, które dzięki elastyczności konfiguracji odpowiadają na potrzeby każdej firmy, niezależnie od jej wielkości. MCX Systems jest w Polsce wyłącznym przedstawicielem koncernu Aastra MATRA Telecom, który w maju br. przejął od EADS Telecom zarządzanie produkcją i dystrybucją systemów telekomunikacyjnych M6500IP oraz NeXspan we wszystkich krajach świata.

... Micromuse ogłosiło że Netia zakupiła i obecnie wdraża pakiet Netcool, służący do zarządzania zdarzeniami dla całej infrastruktury usług IP, ATM oraz Frame Relay. Netia jest największym niezależnym operatorem telefonii stacjonarnej w Polsce świadczącym zintegrowane usługi głosowe i przesyłania danych, jak również hurtowe usługi sieciowe poprzez w pełni cyfrową sieć opartą na technologii światłowodów, której jest wyłącznym właścicielem. Netia spodziewa się, iż pakiet Netcool zwiększy jej wydajność operacyjną, w miarę jak firma będzie skupiała swoją działalność na rosnącym rynku komunikacji biznesowej w Polsce.

... Microsoft poinformował o wprowadzeniu na rynek 64-bitowych wersji Windows Server 2003 oraz Windows XP Professional. Nowe oprogramowanie zapewni użytkownikom wyższą wydajność w zakresie zarządzania danymi, tworzenia zaawansowanych graficznie aplikacji oraz zwiększoną stabilność i bezpieczeństwo działania systemów. Rozwiązania oferują trzydziestodwukrotne zwiększenie pamięci fizycznej oraz tysiąckrotne pamięci wirtualnej, pozwalając na pracę z ogromnymi pakietami danych, bez potrzeby dzielenia ich na mniejsze jednostki. Nowe wersje systemów umożliwią również zwiększenie wydajności w zakresie cyfrowego programowania treści, inżynierii informatycznej, prac naukowo-badawczych oraz rozwoju gier komputerowych.

... NextiraOne została wyróżniona nagrodą dla najlepszego partnera Cisco Systems w roku 2004 w dziedzinie Managed Services w regionie EMEA. NextiraOne została nagrodzona przede wszystkim za zdecydowane ukierunkowanie firmy na oferowanie wysokiej jakości usług.

... Telmax (SPIN) w konsorcjum z Przedsiębiorstwem Informatycznym Kamsoft podpisał umowę na nadzór autorski i konserwację systemu informatycznego Narodowego Funduszu Zdrowia. Wartość kontraktu wynosi 13 246 tys. zł netto. Wszystkie prace mają zostać wykonane do końca bieżącego roku.

... Prezes Urzędu Regulacji Telekomunikacji i Poczty ogłosił rozpoczęcie postępowania przetargowego na trzy rezerwacje częstotliwości z zakresu 3,6–3,8 GHz. Częstotliwości te są przeznaczone do wykorzystania na obszarze całego kraju w służbie radiokomunikacyjnej stałej lądowej (sieci typu punkt-wielopunkt). Mogą być wykorzystywane dla systemów radiowego dostępu abonenckiego w sieciach stacjonarnych (np. dla usług szerokopasmowego dostępu do internetu). Oferty na rezerwację jednej pary kanałów dupleksowych o szerokości 2x3,5 MHz można składać do 15 czerwca br. Każdy uczestnik przetargu może złożyć maksymalnie trzy oferty.

... Veracomp rozszerza portfolio produktów w zakresie bezpieczeństwa. Dystrybutor rozpoczął sprzedaż nowego oprogramowania SurfControl Enterprise Threat Shield do zaawansowanej ochrony przed programami szpiegującymi (spyware). Nowy produkt SurfControl redefiniuje pojęcie ochrony przed złośliwymi aplikacjami. Enterprise Threat Shield blokuje instalację programów szpiegujących na komputerach podłączonych do sieci korporacyjnej.

Opracował Rafał Mikołajczak

System okablowania strukturalnego PowerLink

System okablowania strukturalnego PowerLink firmy ZPAS-NET jest nowoczesnym produktem kablowym do zastosowań teleinformatycznych w nowoczesnych budynkach biurowych i przemysłowych. Różnorodność produktów uwzględniająca wymagania transmisyjne, jak również estetykę użytkową, połączona z rozsądną ceną sprawia, że system ma na rynku coraz większą rzeszę zwolenników. Jest to produkt polski, dostosowany do wymagań rynku lokalnego. Unikatową cechą systemu wyróżniającą go spośród oferty konkurencji jest możliwość realizacji systemów automatyki budynkowej ZPAS M-BUS Control.

Rekomendujemy do tego celu budowę okablowania w oparciu o podsystem PowerVS. Zalecenia ZPAS opracowane w oparciu o normy dotyczące okablowania strukturalnego (EIA/TIA 568B, EN 50173, ISO 11801) pozwalają zaproponować inwestorom nadmiarowe kanały okablowania strukturalnego, które pomimo braku założeń dotyczących budynkowych systemów automatyki (*Building Management Systems* – BMS) w momencie realizacji inwestycji okablowania pozwolą inwestorowi w przyszłości na implementację zaawansowanego systemu automatyki budynkowej w oparciu o istniejące okablowanie strukturalne.

Opis systemu PowerLink

PowerLink jest systemem kablowym zgodnym z normami branżowymi określającymi parametry techniczne dla kategorii 5e, tj. EIA/TIA 568B.2, ISO 11801, EN 50173. Podstawą systemu jest uniwersalne złącze szczelinowe, kompatybilne ze złączami 110 i LSA. Złącza te znajdują się w panelach dystrybucyjnych i gniazdach abonenckich. Można w nim terminować kable narzędziami uderzeniowymi dowolnych producentów. Kable systemowe standardowo dostępne są w powłokach LSOH. Na życzenie oferujemy kable miedziane w powłokach PVC i PE.

Gniazda abonenckie są zrealizowane w oparciu o uniwersalne moduły transmisyjne typu keystone RJ-45

Grupy produktów systemu PowerLink

	Panele	Gniazda		Kable	Standardy
PowerLink 5e	UTP, 19" i 10", prekonfigurowane 1U 8 i 24 RJ45 i 2U 48 RJ45, modularne 1U od 1 do 24 portów RJ45	UTP	prekonfigurowane i modularne natynkowe i powierzchniowe 1 i 2 RJ45, 22,5 45mm i 25 50mm, w gniazdach modularnych moduł transmisyjny typu KEYSTONE	UTP 4-parowe 24 i 26 AWG, PVC, LSOH, PE, kable PE w wersji żelowanej i suchej	kat. 5e – EIA/TIA 568 B.2, klasa D – EN 50173 i ISO 11801 2nd edition
PowerLink TX				UTP 4-parowe 24 AWG, PVC, LSOH	kat. 6 – EIA/TIA 568 B.2, klasa E – EN 50173 i ISO 11801 2nd edition
PowerSafe 5e	STP, 19" i 10", prekonfigurowane 1U 8 i 24 RJ45, modularne 1U od 1 do 24 portów RJ45	STP		FTP, 4-parowe 24 AWG, PVC, LSOH, PE	kat. 5e – EIA/TIA 568 B.2, klasa D – EN 50173 i ISO 11801 2nd edition
PowerSafe TX				FTP, STP SSTP 4-parowe 24 AWG, PVC, LSOH	kat. 6 – EIA/TIA 568 B.2, klasa E – EN 50173 i ISO 11801 2nd edition
PowerVS	UTP, 1U 50 RJ12, 1U 60 par, 3U 150 par	UTP RJ11 i RJ12		25, 50 i 10 par UTP	kat. 3 – EIA/TIA 568 B.2, klasa C – EN 50173 i ISO 11801 2nd edition
OptiLAN	1U, 2U, 3U, 10, 19 i 21" oraz naścienne	ST, S.C., MTRJ, LC, FC-SM i MM oraz E2000		SM 9/125i MM 50/125 i 62,5/15, LSOH, ścisła i luźna tuba oraz uniwersalne	OM1, OM2, OM3: ISO 11801 2nd edition
OptiTEL					

osadzone w płytkach czołowych 22,5 x 45 mm lub 25 x 50 mm z przesłoną przeciwkurzową. W ofercie znajdują się też gniazda w „polskim" standardzie mocowania. Dla wszystkich typów gniazd ZPAS-NET oferuje systemy ramek i puszek natynkowych oraz gniazd elektrycznych mających zastosowanie w dedykowanych instalacjach zasilających.

W małych instalacjach natynkowych przydatne mogą okazać się pojedyncze i podwójne gniazda powierzchniowe RJ-45 UTP kategorii 5e ze złączem RJ bez osłony przeciwkurzowej. Panele dystrybucyjne są skonstruowane w oparciu o specjalnie zaprojektowane obwody drukowane, zapewniające uzyskanie odpowiednich parametrów transmisyjnych przy maksymalnej gęstości połączeń. Kable krosowe wykonane z kabla o przekroju 24 AWG posiadają fabrycznie zaterminowane złącza RJ45, dodatkowo wzmocnione, uformowane w technologii wtrysku tworzyw sztucznych osłony, co powoduje dużą ich giętkość i praktycznie 100-proc. odporność na uszkodzenia mechaniczne.

Bezpieczeństwo danych

W nowoczesnym środowisku biznesowym, podlegającym nieustannym zmianom i modyfikacjom, istotną cechą zabezpieczającą bezawaryjne działanie systemów komunikacyjnych jest niezawodność infrastruktury kablowej. Można ją osiągnąć decydując się na rozwiązania firm posiadających długoletnie doświadczenie w branży, uznanych na rynku, oferujących produkty wysokiej jakości, potwierdzonej certyfikatami niezależnych laboratoriów.

W tym celu firma ZPAS SA powołała w roku 2004 spółkę ZPAS-NET, która skupia wszystkie produkty i kompetencje związane z technologiami informatycznymi i telekomunikacyjnymi. ZPAS-NET jest 100-proc. własnością ZPAS SA i bezpośrednim spadkobiercą długoletnich tradycji ZPAS SA w dziedzinie teleinformatyki i telekomunikacji.

100-proc. gwarancję niezawodności infrastruktury kablowej i bezpieczeństwa danych zapewni jedynie system zainstalowany przez kompetentnych instalatorów, posiadających wysokie kwalifikacje i stosowne uprawnienia producenta.

Autoryzowanymi partnerami ZPAS-NET są najlepsze firmy instalatorskie. Dbamy o ich kompetencje, oferując zaawansowane programy szkoleniowe i wsparcie techniczne.

Autoryzowani Partnerzy ZPAS-NET to firmy zaufane. Jesteśmy przekonani, że gdy zdecydujecie się na ich usługi, potwierdzą swój profesjonalizm podczas prac instalacyjnych.

Rękojmią bezpieczeństwa użytkownika systemu kablowego oprócz wysokiej jakości produktów i profesjonalnego serwisu jest gwarancja systemowa. Procedura uzyskania gwarancji systemowej ZPAS-NET jest nieskomplikowana, a klient decyduje o okresie jej obowiązywania. Gwarancją mogą być objęte instalacje wykonane przez firmy posiadające Autoryzację ZPAS-NET. Maksymalny okres to 25 lat, a minimalny to 5 lat. System gwarancji systemowych ZPAS-NET umożliwia przedłużenie pierwotnego okresu gwarancyjnego na dalsze lata. Po upływie okresu gwarancji wystarczy zgłosić chęć przedłużenia gwarancji. Po dokonaniu przez specjalistów ZPAS-NET przeglądu instalacji gwarancja jest przedłużana na kolejne 5 lat. Procedurę tę użytkownik instalacji może powtarzać wielokrotnie aż do momentu fizycznego demontażu okablowania. Jest to możliwość dająca uzyskanie gwarancji niezawodnego działania na cały czas użytkowania okablowania.

ZPAS-NET jako producent elementów okablowania strukturalnego dopuszcza w instalacjach certyfikowanych zastosowanie kabli liniowych firmy MADEX oraz miedzianych i światłowodowych kabli teleinformatycznych firmy DRAKA Multimedia Cables Niemcy. Wszystkie kable firmowane logo ZPAS pochodzą z fabryk firmy DRAKA. Jednocześnie ZPAS-NET jest jednym z dwóch dystrybutorów pełnej oferty kablowej firmy DRAKA, w tym kabli współosiowych, przemysłowych i specjalnych. Więcej informacji dotyczących systemu znajduje się na stronach internetowych www.zpas.net.

Dział marketingu ZPAS-NET

Obudowy teleinformatyczne ZPAS SA

W niniejszym artykule przedstawiam ogólną klasyfikację obudów produkowanych przez ZPAS SA. Ponieważ szczegółowo zajmuję się tylko wybranymi wyrobami, dlatego zachęcam do zapoznania się z pełną ofertą umieszczoną na naszych stronach internetowych www.zpas.pl. Na podanych stronach znajdują się równocześnie dane kontaktowe do naszych pracowników, którzy w przypadku konkretnych potrzeb klientów mogą udzielić dodatkowych wyjaśnień i porad technicznych. Nie omawiam m. in. grupy obudów energetycznych (stanowiącej odrębną gałąź w klasyfikacji obudów ZPAS), stojaków (obudów o konstrukcji otwartej), obudów wiszących i wyposażenia dodatkowego. Skupiam się natomiast na obudowach stojących, stanowiących dominującą kategorię produkowanych w ZPAS SA urządzeń zabezpieczenia teletechnicznego oraz pokrótce wspominam o szafkach SD i SJ.

Obudowy teleinformatyczne produkowane w ZPAS SA można podzielić na trzy grupy: szafy stojące, szafki wiszące i stojaki (racki). W grupie szaf stojących w obecnej ofercie produkcyjnej znajdują się: standardowe szafy SZB 19", szafy SZBk 19" zgodne z wymogami EMC, szafy komputerowe SZB PC 19", szafy serwerowe SZB SE 19", szafy kolokacyjne DSR 19" oraz szafy telekomunikacyjne (SZT 21", SZT-1 19"/21", SZT-2 19"). Do obudów stojących zaliczyć należy również stojaki dwuramowe (SRD 19") i jednoramowe (SRS 19" i SRC 19"), których jednak nie będę omawiał.

Obudowy teleinformatyczne – szafy stojące SZB

Podstawowa, uniwersalna **szafa teleinformatyczna SZB** przeznaczona jest do zastosowania wewnątrz pomieszczeń. Oferowana jest w 44 wykonaniach gabarytowych (w tym 17 jest dostępnych w stałej sprzedaży z magazynu ZPAS), w wysokościach od 15 U do 45 U. Szerokości i głębokości tych szaf wykonywane są jako kombinacja dwóch wielkości: 600 i 800 mm. Szafy SZB posiadają rozbudowany system konfiguracji dotyczący również możliwości wyposażenia w różne wykonania drzwi, osłon i tzw. dachów. Szafy przystosowane są do montażu szeregowego (zespołowego), a konstrukcja szaf pozwala na doprowadzenie kabli z dowolnej strony także przy takim rodzaju zabudowy.

Szafy standardowo wyposażane są m.in. w cztery belki nośne o rozstawie 19", niemniej w szafach o szerokości 800 mm istnieje możliwość ustawienia belek nośnych w rozstawie 21". Obudowy te posadowione mogą być

Fot. 1. Szafa SZB o szer. 600 mm z drzwiami przednimi blaszanymi z szybą szklaną i zamkiem baskwilowym

na kółkach lub regulowanych stopkach albo na cokołach prostych lub z możliwością poziomowania. W ZPAS SA produkowane są również wykonania niestandardowe szaf, gdzie rozwiązania konstrukcyjne są dostosowywane do potrzeb klienta, jednak możliwość zmian wymaga wcześniejszych konsultacji z naszymi pracownikami. Informacje dotyczące zakresu dostawy i wyposażenia dodatkowego znajdują się na naszych stronach internetowych.

Jako uzupełnienie przybliżę niektóre dane techniczne szaf SZB. Szkielet i belki nośne wykonane są z blachy stalowej o grubości 2,0 mm, osłony boczne i drzwi bez szyby z blachy stalowej 1,0 mm, natomiast przy drzwiach z szybą metapleksową grubość blachy wynosi 1,5 mm, a w przypadku drzwi blaszanych z szybą ze szkła hartowanego wielkość ta wynosi 2,0 mm. Przy zastosowaniu drzwi szklanych grubość szkła (hartowanego) wynosi 6,0 mm. Stopień ochrony dla tych szaf jest na poziomie IP 20 (zgodnie z normą PN 92/E-08106/EN 60529 / IEC 529), ale może być podwyższony do IP 41. Szkielet, dach, osłony, drzwi i cokół malowane są w standardzie farbą proszkową o grubej strukturze w kolorze RAL 7035, jednak po uzgodnieniu możliwe jest wykonanie szaf w innym, dowolnym kolorze z kata-

logu RAL. Belki nośne wykonuje się z alucynku, natomiast niektóre elementy (np. wysięgniki) są ocynkowane.

Szafy stojące SZBk, SZB PC, SZB SE i DSR

Powyżej dość szczegółowo przybliżyłem uniwersalne szafy SZB, ponieważ inne grupy szaf bazując na konstrukcji SZB stanowią rozwiązania pochodne. Omawiając inne szafy kategorii SZB skupię się więc na różnicujących je właściwościach i rozwiązaniach konstrukcyjnych.

Wersją najbardziej zbliżoną do szaf SZB są szafy **SZBk 19"** zgodne z wymogami EMC. Głównym zadaniem tych obudów jest ekranowanie urządzeń emitujących fale elektromagnetyczne. Szafy te produkowane są w 24 wykonaniach i w porównaniu z szafami standardowymi mają trochę zawężony zakres wyposażenia podstawowego, co wynika z konieczności spełnienia wymogów EMC. Inne właściwości pozostają bez zmian, np. możliwość wyposażenia w odpowiedni system wentylacyjny czy systemy doprowadzania kabli. Szafy te przeszły badania na skuteczność ekranowania i posiadają certyfikat Instytutu Telekomunikacji i Akustyki Politechniki Wrocławskiej oraz certyfikat Agencji Bezpieczeństwa Wewnętrznego w Warszawie.

Szafy **SZB PC** produkowane są w 16 wykonaniach w zakresie wysokości od 36 U do 45 U. Podobnie jak szafy SZBk, są one w znacznym stopniu oparte na konstrukcji podstawowej SZB, co pozwala na pełną kompatybilność montażu urządzeń i wyposażenia dodatkowego dla standardu 19". Cechą szczególną tej grupy jest podział przestrzeni wewnętrznej obudowy na dwie komory, poprzez rozdzielenie konstrukcji półką na klawiaturę komputera.

Fot. 2. Szafa SZB PC o szer. 600 mm z drzwiami przednimi blaszanymi z szybą szklaną

Fot. 3. Szafa SZB SE o szerokości 600 mm z drzwiami przednimi szklanymi

Szafy serwerowe SZB SE 19" są obudowami zapewniającymi ochronę sprzętu zainstalowanego w serwerowniach. Oferowane są w 14 wykonaniach gabarytowych. Szafy te cechuje rozbudowany system konfiguracji osłon, drzwi i tzw. dachów. Pozwala to np. na projektowanie i kontrolowanie drogi strumienia wentylacyjnego wewnątrz urządzeń, czemu pomagają inne niż w przypadku szaf SZB rozwiązania w zakresie perforacji osłon i drzwi. W przypadku szaf serwerowych należy wskazać na dość istotne różnice konstrukcyjne w odniesieniu do standardu SZB: wysuwaną ramę wsporczą w cokole (zabezpieczającą przed przechylaniem szafy podczas wysuwania zabudowanych ciężkich urządzeń, np. serwerów), montaż 6 belek nośnych czy jedną dla wszystkich wykonań głębokość całkowitą szaf 1000 mm. Szafy SZB SE posiadają także odmienny system otworowania płyt dolnych i górnych, co stwarza dużo większe możliwości montażowe przy zabudowie urządzeń.

Szafy kolokacyjne DSR 19" pozwalają na umieszczenie w jednej szafie kilku niezależnych serwerów. Ich zadaniem jest ochrona zainstalowanych urządzeń przy jednoczesnym zapewnieniu właściwej wentylacji. Szafy te wykonuje się w 6 wariantach podziału przestrzeni do zabudowy. Drzwi przednie i tylne wykonywane są z bla-

Fot. 4. Szafy DSR w zabudowie szeregowej

chy stalowej perforowanej w trzech wysokościach: 47 U, 23 U, 11 U, przy czym z tyłu szafy zamiast kilku drzwi można zamontować jedną osłonę na całej wysokości szafy. Standardowo z boku szaf przewidziano zastosowanie osłon perforowanych, które w przypadku zabudowy szeregowej mogą pełnić funkcję przegrody. Drzwi i osłony wyposażane są w zamki jednopunktowe bez klamki, jednak na życzenie klienta można zastosować inne zamki. Poszczególne przedziały szafy oddzielane są za pomocą mocowanych do szkieletu poziomych przegród. Każdy z tych przedziałów posiada niezależny stelaż 19" i wydzielone kanały kablowe biegnące po

Fot. 5. Szafka SD o wysokości 10 U z drzwiami szklanymi – widok z przodu

Fot. 6. Szafka SJ o wysokości 10 U z drzwiami szklanymi

obu stronach obudowy. Wprowadzenia kabli do szafy można dokonać od góry lub od dołu.

Obudowy teleinformatyczne – szafki wiszące

Grupa obudów wiszących obejmuje: szafki SKI 10", szafki SD 19", szafki SJ 19" oraz szafki SWT 19"/21". Szafki wiszące dwusekcyjne SD 19" (dostępne w 5 wysokościach od 6 U do 18 U), podobnie jak wersja jednosekcyjna SJ 19" (dostępne w 6 wysokościach od 4 U do 18 U), przeznaczone są do zastosowania wewnątrz pomieszczeń. Konstrukcyjnie szafki SD składają się z dwóch sekcji, umożliwiając „otwieranie" szafki na łączeniu sekcji, co umożliwia dostęp z boku do urządzeń zamontowanych wewnątrz (patrz fot.). Głębokość całkowita szafek SD wynosi 500 mm. Wersja jednosekcyjna SJ wykonywana jest w dwóch głębokościach, 400 i 600 mm.

Standardowo szafki wyposażone są w dwa kątowniki nośne w rozstawie 19" z płynną regulacją położenia, zaślepki pełne i przepust szczotkowy. Materiałem podstawowym jest blacha stalowa (korpus o gr. 1,25 mm, osłona tylna 0,8 mm, kątowniki nośne 1,5 mm, zaślepki pełne i drzwi blaszane 1,0 mm), przy czym drzwi przednie mogą być blaszane lub ze szkła hartowanego o gr. 4,0 mm. Wykończenie powierzchni podobne jak w szafach stojących. Stopień szczelności szafek SD i SJ wynosi IP 30 (PN 92/E-08106/EN 60 529/IEC 529). Podobnie jak w przypadku obudów stojących, do szafek dostępny jest szeroki zakres elementów wyposażenia dodatkowego: półki, szuflady, zespół wentylacyjny, listwy zasilające itd.

Krzysztof Karwowski
specjalista ds. PR i reklamy ZPAS SA

Zasilanie awaryjne

Firma Eaton jest producentem rodziny zasilaczy bezprzerwowych (UPS) Powerware 9315. Menedżerowie działów informatyki i administratorzy obiektów mogą korzystać obecnie z modeli o mocach 300/400 kVA i współczynniku mocy na wyjściu 0,9, dostępnym wcześniej tylko w modelach o mocy 625 kVA. Każdy z modeli z rodziny 9315 może współpracować online poprzez sieć ethernet lub internet z systemami zdalnego monitorowania i zarządzania.

Większa moc czynna na wyjściu Powerware 9315 to trójfazowy zasilacz bezprzerwowy online z systemem podwójnej konwersji, posiadający wysoko wydajne i zaawansowane możliwości komunikacyjne z systemami informatycznymi o krytycznym znaczeniu dla przedsiębiorstwa. Dla przykładu, nowy współczynnik mocy na wyjściu modelu 9315 400 kVA oznacza zwiększenie mocy czynnej na wyjściu z 320 do 360 kW, co czyni z niego odpowiedni system dla centrów przetwarzania danych następnej generacji, stosujących serwery mogące wykorzystać wyższy współczynnik mocy.

Współczynnik mocy wyjściowej 0,9 to realny wzrost mocy użytecznej bez zwiększania powierzchni zajmowanej przez zasilacz, a więc ujmując to inaczej – wzrost mocy użytecznej w przeliczeniu na powierzchnię zajmowaną przez zasilacz. Ta cecha sprawia, że menedżerowie działów informatyki i administratorzy obiektów mają większą swobodę w zarządzaniu obciążeniem i planowaniu zagospodarowania obiektów.

Zasilacze bezprzerwowe z rodziny 9315 wyposażone są również w technologię podwójnej konwersji online, która eliminuje anomalie zasilania i zapewnia wysoki poziom bezpieczeństwa na poziomie niemal 100 proc. czasu użytecznego, chroniąc dołączone serwery, urządzenia pamięci masowej, sprzęt sieciowy i urządzenia medyczne.

Powerware 9315 to rozwiązanie w zakresie zarządzania energią, które gwarantuje stabilne, zgodne z normami zasilanie systemów o krytycznym znaczeniu w bankowości, placówkach służby zdrowia, administracji publicznej i środowiskach korporacyjnych.

Rozszerzone możliwości komunikacji w sieci

Niezależnie od podwyższonego współczynnika mocy 0,9, wersja 9315 została wyposażona w zintegrowane gniazdo komunikacyjne X-Slot. Zwiększa to możliwości komunikacyjne zasilacza UPS poprzez umożliwienie obsługi różnorodnego oprogramowania oraz aplikacji komunikacyjnych, w tym:

- ✔ umożliwia bezpośrednią integrację informacji z UPS (pomiary i status) z systemem zarządzania budynkiem, korzystającym z protokołu Modbus RTU,
- ✔ umożliwia zdalne monitorowanie za pośrednictwem standardowej przeglądarki internetowej, poczty elektronicznej lub systemu zarządzania siecią, korzystającego z protokołu SNMP.

Gniazdo X-Slot jest zasilane z UPS, co zapewnia niezawodną komunikację w razie awarii, zaś funkcja *hot swap* ułatwia instalację opcji komunikacyjnych.

Powerware 9315 zaprojektowano z zastosowaniem nadmiarowych komponentów o krytycznym znaczeniu, minimalnej liczbie płytek drukowanych, w pełni cyfrowego przetwarzania sygnału oraz doskonałego chłodzenia.

Zasilacze Powerware 9315 można łączyć równolegle, zarówno dla uzyskania nadmiarowości, jak i zwiększenia mocy, korzystając z opatentowanej technologii Powerware Hot Sync UPS. Technologia Powerware Hot Sync umożliwia pracę dwóch lub więcej modułów UPS w tandemie bez łączącej je plątaniny kabli. Tego rodzaju bezprzewodowe rozwiązanie oznacza, że jednostki pracują synchronicznie, nawet jeśli pracują niezależnie od siebie. Gdy jeden z modułów ulegnie awarii, druga jednostka natychmiast przejmuje obciążenie, nie dopuszczając do załamania sieci. Nadmiarowość typu N + 1 zapewnia dodatkowy stopień niezawodności, jednocześnie eliminując pojedyncze punkty awarii, spotykane w innych równoległych systemach nadmiarowych, stosowanych w przemyśle.

Powerware 9315 UPS

Podobnie jak inne modele z rodziny zasilaczy Powerware 9xxx, zasilacz 9315 zapewnia całkowitą ochronę przed wszystkimi dziewięcioma powszechnie spotykanymi problemami zasilania, a więc zanikiem napięcia, spadkiem mocy, przepięciami, zaniżonym lub zawyżonym napięciem, przejściowymi zakłóceniami przebiegu napięcia/prądu, szumami, wahaniami częstotliwości oraz zniekształceniami harmonicznymi.

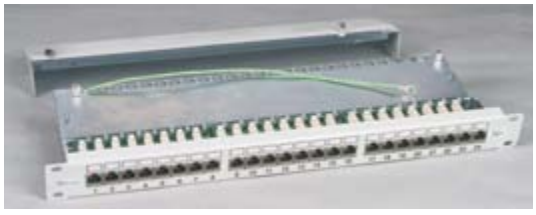
Opracowano na podstawie materiałów firmy Eaton

System okablowania strukturalnego Xpatch

MOELLER

Jednym z podstawowych elementów sieci lokalnych i korporacyjnych jest okablowanie strukturalne. Okablowanie miedziane czy światłowodowe jest częścią sprzętową całego systemu przesyłu danych. W oparciu o medium miedziane obecnie budowane są sieci złożone z osprzętu kategorii 6 umożliwiającego budowę łączy i kanałów klasy E.

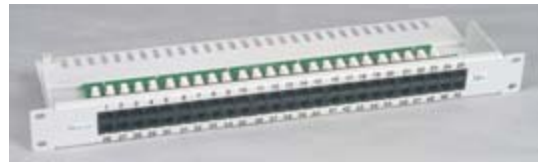
Firma Moeller posiada w swojej ofercie system sieciowy Xpatch. Na system ten składają się obudowy teleinformatyczne oraz elementy pasywne sieci, takie jak: panele krosowe (patchpanele), kable teleinformatyczne (skrętki 4-parowe), kable krosowe (patchkable), gniazdka podłączeniowe i osprzęt. Wszystkie elementy pasywne okablowania strukturalnego dostępne są w dwóch rodzajach: w wersji ekranowanej (FTP, SFTP, STP, CSTP) oraz nieekranowanej (UTP). Sieć zbudowana z elementów ekranowanych jest mniej podatna na zakłócenia (zarówno obce, jak i własne) i umożliwia maksymalne wykorzystanie parametrów sieci (szybkość, pasmo, odległość), natomiast elementy nieekranowane są tańsze. Panele krosowe mogą być w wersji standardowej – każdy panel posiada 16 lub 24 portów RJ45 lub w wersji modułowej, gdzie każde gniazdo RJ (RJ11, RJ12, RJ45 UTP i FTP) montowane jest oddzielnie (rys. 1a i 1b). Wersja modułowa pozwala na bardzo łatwe rekonfigurowanie torów oraz na dokładne dopasowanie liczby modułów do potrzeb. Moduły RJ dostępne są oddzielnie, a terminowanie modułu wykonuje się w systemie IDC (wciskowy – wymagana zaciskarka).



Rys. 1a. Panel krosowy 1U, 24-portowy ekranowany kat. 6

Rys. 1b. Panel krosowy modułowy 1U, ekranowany wraz z ekranowanymi modułami kat. 5 (5e)

Wersje standardowe paneli krosowych terminowane są za pomocą złączy LSA (specjalne narzędzie wciskowe LSA). Panele krosowe telefoniczne (kat. 3, ISDN) przy wysokości 1U mieszczą 25 lub 50 gniazd (rys. 2).



Rys. 2. Panel krosowy telefoniczny 1U 50 gniazd RJ45

Kable teleinformatyczne – 4x2xAWG24/23/22 wykonane są w różnych kategoriach – 5 (5e), 6 i 7 (1200 MHz) (rys. 3). Ich powłoki w zależności od wersji wykonane są z PVC lub jako niskodymne i niepalne:

Rys. 3. Przekrój kabla CSTP (podwójny ekran) kat. 7 (1200 MHz)

LSOH i FRNC. Również tu mamy wybór spośród wersji ekranowanych (FTP, SFTP, STP, CSTP) i nieekranowanych (UTP). Wykorzystuje się je głównie do okablowania strukturalnego pionowego i poziomego – pomiędzy rozdzielnicami piętrowymi oraz od rozdzielnic do gniazdek. Także kable krosowe dostępne są w pełnej palecie wykonań oraz kolorów (ważne dla instalatorów). Kolory wykonań to szary (podstawowy), czerwony, niebieski, zielony, żółty (rys. 4). Do specjalnych zastosowań możemy wykorzystać kabel „crossover" – krosujący tory (w ramach torów złącza

Rys. 4. Kable krosowe kat. 5 (5e) UTP i 6 STP

RJ45). Długość kabli krosowych można dobrać wg ciągu: 0,5; 1; 1,5; 2; 2,5; 3; 4; 5; 7; 10 m.

Gniazdka podłączeniowe wykonywane są w kat. 5 (5e) i 6 jako ekranowane 2xRJ45 w wersji podtynkowej (rys. 5). W ofercie jest również puszka natynkowa do gniazdka. Puszka i gniazdo dostępne są w dwóch kolorach: kremowym i śnieżnobiałym.

Rys. 5. Gniazdo 2xRJ45 ekranowane

W oparciu o wymienione komponenty można budować zarówno proste sieci teleinformatyczne, jak i sieci rozległe, np. wielobudynkowe.

Samo użycie odpowiedniej jakości komponentów nie wystarcza do tego, by sieć spełniała odpowiednią klasę. Należy przestrzegać reguł i zaleceń dotyczących samej instalacji urządzeń (a w szczególności układania kabli). Pamiętajmy o tym, że instalując w nieodpowiedni sposób nawet najlepsze komponenty nie wykorzystamy w pełni ich możliwości.

Nowością w ofercie są szafki naścienne 19" **Xpatch Basic Line** (fot. 6). Ich atutem jest dobra cena finalnego produktu, która została uzyskana poprzez zoptymalizowany system produkcyjny. Szafki mają możliwość zabudowy od 6 U do 18 U i występują w dwóch wersjach: jedno- i dwusekcyjne. Dostępna jest także nowa linia szaf stojących **Basic Line NCE** (fot. 7) o pojemności od 23 U do 46 U. Konstrukcja ramowa pozwala na duże obciążenie szafy. Dzięki symetryczności z trzech stron stosuje się te same elementy do zabudowy: ściana pełna lub z drzwiami metalowymi na boki i tył szafy. Szafy standardowe oferowane są w wielu wariantach wykonań. W ofercie Moeller'a

Fot. 6. Szafka naścienna NWE Basic Line

Fot. 7. Szafa stojąca NCE Basic Line

znajdują się także **szafy serwerowe** (fot. 8) o głębokości 1000 mm (wys. 42 U i 46 U, szer. 600 mm i 800 mm). Są one bogato wyposażone i przygotowane do instalowania serwerów komputerowych. Szafy te oferowane są w kolorze czarnym RAL 9005.

Fot. 8. Szafa serwerowa

Bogaty osprzęt dodatkowy, taki jak: cokoły, szyny, listwy montażowe, uchwyty i wieszaki kablowe, panele zaślepiające, półki, listwy zasilające, specyfikowane oświetlenie i wentylacja umożliwiają dostosowanie zabudowy szaf do indywidualnych potrzeb.

Adam Własowski
Product Manager Moeller Electric

Sieć bezprzewodowa klasy biznesowej: ORiNOCO AP4000 i AP700 Proxim

Punktem dostępowym o największych możliwościach i wytyczającym nowe standardy jakości w technologii WLAN jest ORiNOCO AP4000 firmy Proxim.

AP4000 jest pierwszym punktem dostępowym posiadającym wbudowane radio obsługujące wszystkie trzy standardy radiowe: 802.11a, 802.11b oraz 802.11g jednocześnie. Posiada wszystkie funkcjonalności niezbędne w nowoczesnej sieci bezprzewodowej, obsługuje najnowsze standardy bezpieczeństwa oraz ma możliwość dołączenia anten zewnętrznych Dual Band, działających w paśmie 2,4 oraz 5,15-5,25 GHz poprzez dedykowane konektory. AP4000 zapewnia wyższą wydajność przy jednoczesnej pracy klientów radiowych: do 40 Mbit/s przepływności w czasie jednoczesnej pracy klientów 802.11g i 802.11a. AP4000 potrafi obsługiwać wiele grup roboczych przy różnych mechanizmach bezpieczeństwa dla każdej z nich: tak by pracownicy, goście oraz podwykonawcy firmy mogli łatwo i bezpiecznie korzystać z firmowej infrastruktury IT. Dzięki stałemu rozwijaniu funkcjonalności przez firmę Proxim AP4000 obsługuje najnowsze standardy wzajemnej autentykacji WPA2, TKIP, 802.1x (PEAP, TTLS, TLS, SIM), dynamiczne, zmienne klucze szyfrujące zmieniane per użytkownik/sesja/czas, oraz szyfrację AES, protokoły 802.11i, 802.11e (Wireless Multimedia – QoS). Dzięki rozwijanym protokołom transmisji głosu w sieciach bezprzewodowych już można stosować w firmowych sieciach rozwiązania typu *voice over wireless*: VoWLAN. Zdalne administrowanie może być w pełni bezpieczne dzięki szyfrowaniu sesji HTTPS (SSL), SSH lub poprzez SNMPv3 oraz niekłopotliwe nawet przy aktualizacji oprogramowania: stary firmware AP jest kasowany nie podczas aktualizacji, ale po poprawnym uruchomieniu nowego. Również dokonanie lokalnego resetu przez nieupoważnioną osobę nie musi spowodować skasowania konfiguracji, ponieważ po restarcie AP pobierze nowy plik konfiguracyjny ze zdefiniowanej lokalizacji w sieci. Sugerowana cena detaliczna AP4000 wynosi 2140 zł netto.

Wszystkie możliwości AP4000 są także dostępne w mniejszym **AP700**, który różni się od AP4000 jedynie konfiguracją interfejsów radiowych: AP700 może pracować w trybie 11a lub 11b/g. Sugerowana cena detaliczna AP700 wynosi 1481 zł netto.

Tsunami MP.11a/MP.11a R: systemy topologii punkt-wielopunkt

Tsunami MP.11a przeznaczony jest do transmisji danych dla wielu zastosowań, takich jak: szerokopasmowy dostęp do internetu, łączenie segmentów sieci LAN firm czy monitoring wizyjny w technologii video IP. Umożliwia też w prosty sposób rozszerzenie sieci lokalnej, tworząc sieć radiową o zasięgu do ok. 12 km od stacji bazowej. Wersja zewnętrzna Tsunami MP.11a R umożliwia osiąganie większych zasięgów od wersji MP.11a z uwagi na eliminację długich kabli niskostratnych, silnie tłumiących sygnał 5GHz.

Tsunami MP.11a – wersja do montażu wewnętrznego

Tsunami MP.11a R – wersja do montażu zewnętrznego

Rodzina Tsunami MP.11a składa się z 3 urządzeń niewymagających żadnych modułów. Jest to stacja bazowa BSU (wymagana do działania linku) oraz dwa rodzaje urządzeń odbiorczych: stacja odbiorcza SU oraz rezydentna stacja odbiorcza RSU, będąca tańszą wersją SU obsługującą 8 adresów MAC na interfejsie Ethernet. Tsunami MP.11a R składa się również z 3 kompletnych urządzeń: stacji bazowej BSU-R oraz dwóch rodzajów stacji odbiorczych: SU-R w wersji ze zintegrowaną anteną 23dBi oraz SU-A bez anteny, ale złączem radiowym N. Według własnych wymagań należy dobrać kable niskostratne oraz anteny.

Tsunami MP.11a należy do najefektywniejszych systemów radiowej transmisji danych w pasmach wolnych od opłat z uwagi na unikatowy, opracowany przez firmę Proxim protokół WORP: Wireless Outdoor Router Protocol. Dzięki WORP systemy transmisyjne Proxim działają stabilniej, zapewniają większy zasięg, większą realną przepustowość oraz możliwość jednoczesnej obsługi znacznie większej liczby urządzeń klienckich niż standardowe urządzenia WLAN stosujące protokoły 802.11. Wzrost wydajności osiągnięto dzięki zastosowaniu mechanizmów multipleksowania danych polegających na gromadzeniu pakietów IP w powiększonych ramkach warstwy drugiej, dzieleniu ich i przesyłaniu jednorazowo w ramkach WORP zbliżonych maksymalnie do rozmiaru 2304 bajtów. Mechanizm ten zmniejsza udział nagłówków IP w transmisji ogółem, co skutkuje znacznym zwiększeniem rzeczywistych transferów. W samym protokole WORP zawarte są mechanizmy symetrycznego oraz asymetrycznego sterowania przepływnością, uwierzytelniania stacji protokołem MD5-CHAP, natomiast transmisja jest szyfrowana algorytmem AES z kluczem 128-bitowym.

Kluczowe funkcjonalności Tsunami MP.11a/MP.11a R

Protokół WORP	superpakietowanie oraz fragmentacja pakietów, zarządzanie pasmem
250 stacji na BSU	jedna stacja bazowa BSU lub BSU-R obsługuje do 250 stacji odbiorczych
DDRS	dynamiczna negocjacja prędkości pracy na podstawie sygnału radiowego
Roaming SU	przełączanie SU do zapasowego BSU w wypadku awarii głównej stacji bazowej, mobilne SU mogą przełączać się między BSU do 200 km/h
DFS, TPC	dynamiczna selekcja kanału pracy, kontrola mocy emitowanej co 3dB
Bridge/router	tryb bridge, router (RIPv1/ RIPv2), NAT, DHCP (client/server/relay)
Bezpieczeństwo	szyfrowanie transmisji AES, autentykacja stacji/klientów RADIUS, intra-cell block, tworzenie do 16 podgrup stacji, filtrowanie pakietów, Access List
Log temperatury	logowanie temperatury wewnętrznej urządzenia (tylko MP.11a R i QB.11a R)
No-sleep mode	priorytetyzacja wybranych stacji odbiorczych (tylko MP.11a R i QB.11a R
54 i 48 Mbit/s	wyższe radiowe prędkości pracy: 54 i 48 Mbit/s (tylko MP.11a R* i QB.11a R)
QoS, VLAN	sprzętowe wsparcie QoS oraz VLAN, obsługa po aktualizacji firmware*

* plany rozwojowe Q2/Q3 2005

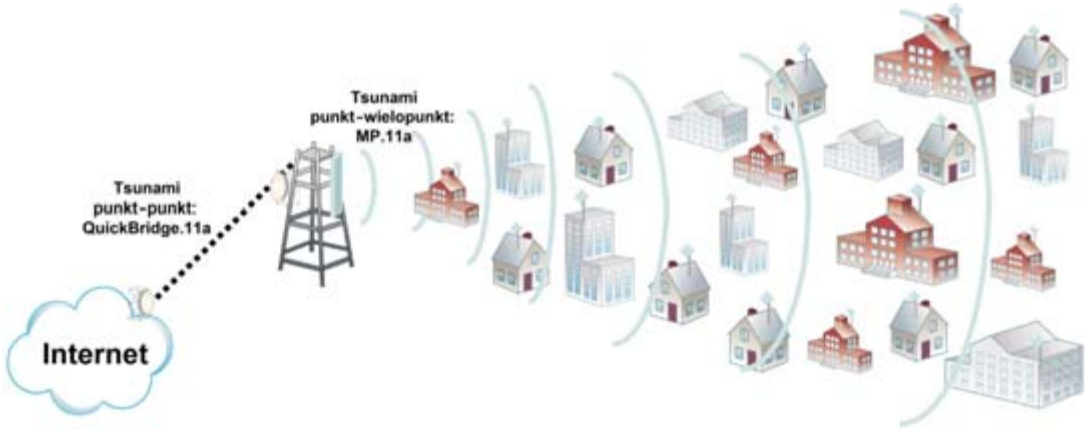
Tsunami QuickBridge.11a R: system topologii punkt-punkt

Tsunami QuickBridge.11a R jest zmodyfikowaną wersją Tsunami MP.11a dedykowaną do szybkiego tworzenia radiowych połączeń punkt-punkt.

System jest oferowany w kompletnym zestawie składającym się ze stacji bazowej (QB-BSU-R), stacji klienckiej (QB-SU-R), dwóch sztuk zewnętrznego kabla Ethernet z wodoszczelnymi końcówkami w odcinkach po 50 metrów, dedykowanych zasilaczy PoE oraz zestawów montażowych. Obydwie stacje QB.11a R posiadają zintegrowane anteny dualnej polaryzacji o zysku energetycznym 23 dBi, są przystosowane do pracy w zakresie temperatur od –33 do +60 stopni Celsjusza oraz są gotowe do montażu zaraz po wyjęciu z pudełka dzięki fabrycznej prekonfiguracji zestawu.

Najistotniejszą zaletą QuickBridge.11a R jest jego zgodność z MP.11a R – oznacza to, że **QB.11a R można rozbudować do topologii punkt-wielopunkt.** W konfiguracji stacji bazowej QB-BSU-R zmienia się jej tryb pracy na SU i wówczas obydwa urządzenia (baza QB.11a oraz jej stacja odbiorcza) stają się stacjami odbiorczymi MP.11a, które będą współpracować z dowolną stacją bazową: wewnętrzną BSU lub zewnętrzną BSU-R.

Zdecydowana większość sieci radiowych zaczynała od pojedynczych połączeń punkt-punkt, które w następstwie organicznego wzrostu sieci rozwijały się do rozbudowanych systemów punkt-wielopunkt. Obydwa systemy mogą współpracować w sieci radiowej, przykład aplikacji przedstawiamy poniżej:



Dodatkowe informacje oraz ceny dostępne są na www.veracomp.pl/tsunami. Firma Veracomp proponuje swoim Partnerom przystąpienie do Programu Partnerskiego Proxim, dającego dodatkowe korzyści oraz specjalne ceny. Szczegóły na stronach Centrum Edukacyjnego Compendium: www.compendium.pl.

Usługa podnosząca wydajność sieci klienckich

Firma BT wprowadziła nową usługę umożliwiającą klientom biznesowym na całym świecie nadawanie priorytetu przesyłowi głosowemu, multimedialnemu i danych, które funkcjonują równocześnie w sieciach konwergentnych. Nowa usługa, Six Class of Service Differentiated Services Code Point (6 CoS DSCP) gwarantuje wydajność aplikacji przez nadanie priorytetu usługom komunikacyjnym w ramach sześciu odrębnych klas usług, dzięki czemu możliwe jest dostosowanie się do przyszłych wymagań sieci korporacyjnych.

– W miarę jak coraz więcej przedsiębiorstw zaczyna korzystać z uwarunkowanych czasowo usług związanych z przesyłem głosu i obrazu przez wirtualne sieci prywatne korzystające z technologii MPLS IP, rośnie znaczenie klas usług (Classes of Service) i sieci inteligentnych, które mogą przypisywać pierwszeństwo kluczowym aplikacjom. Wprowadzenie w sieciach BT sześciu klas usług podnosi standardy rynkowe. Takie rozwiązanie docenią klienci, którzy przed podłączeniem swojej sieci do infrastruktury sieciowej dostawców usług informatycznych i komunikacyjnych oczekują najwyższej gwarancji wydajnego działania kluczowych aplikacji – twierdzi **Sandra O'Boyle** z firmy konsultingowej Current Analysi.

Aby spełnić zróżnicowane wymagania klientów dotyczące jakości usług QoS, nowy produkt jest zgodny ze standardem DSCP, który został zaprojektowany z przeznaczeniem dla nowoczesnych sieci i udoskonala rozwiązania QoS przez umożliwienie klientom wyboru poziomu funkcjonowania w zależności od danego pakietu przez zaznaczenie określonej wartości pola DSCP w nagłówku pakietu IP. To rozszerzenie wcześniejszej oferty BT 3CoS zostało wprowadzone w związku ze wzrastającym użytkowaniem bardziej zaawansowanych aplikacji, takich jak ERP (*Enterprise Resource Planning*), telefonia korzystająca z protokołu IP i aplikacje strumieniowe wideo.

– W dzisiejszej cyfrowo usieciowionej gospodarce firmy coraz częściej używają wysoko zaawansowanych aplikacji danych działających w czasie rzeczywistym – między innymi zaawansowanej komunikacji głosowej i video przez protokół IP. Nowa usługa, 6CoS DSCP, jest odpowiedzią BT na zapotrzebowanie klientów na technologię konwergentnych danych i komunikacji, pozwala im ona również przygotować się na długoterminowe wymagania związane z funkcjonowaniem aplikacji (6CoS DSCP nie posiada ograniczeń modeli 3 lub 4 klasy ani nie jest tak złożony, jak usługi posiadające więcej niż sześć poziomów klas) – uważa **Aaron McCormack**, wiceprezes BT Global Products.

Model 6CoS DSCP BT oferuje również większą elastyczność i skalowalność, umożliwiając klientom końcowym przełączanie się pomiędzy klasami bez dokonywania skomplikowanej konfiguracji. Zwiększona przejrzystość w oznaczaniu pakietów umożliwia klientom łatwiejsze wdrożenie schematu w ich środowisku, co obniża łączne koszty posiadania informatyki (*total cost of ownership, TCO*) i udoskonala funkcjonowanie aplikacji. Konsumenci mogą na przykład dostroić swoją sieć, aby sprostać wymaganiom aplikacji głosowych i danych czy też mogą posiadać opcjonalną, dedykowaną klasę multimedialną do korzystania z aplikacji wideo.

W przeciwieństwie do usług oferowanych przez konkurencyjne firmy, nowa usługa 6CoS DSCP działa zarówno w sieciach nadrzędnych, jak i podrzędnych. Funkcjonowanie usługi 6CoS DSCP w sieci nadrzędnej zapewnia przedsiębiorstwom doskonałe funkcjonowanie ich uwarunkowanych czasowo aplikacji nawet w przypadku niespodziewanych, nagłych zmian w profilach ruchu sieciowego. Sieć aplikacji utrzymuje nadane priorytety nawet w sytuacjach awarii poprzez przekierowanie ruchu sieciowego.

BT jest jednym z wiodących światowych dostawców rozwiązań komunikacyjnych. Firma obsługuje klientów w Europie, obu Amerykach, regionie Azji i Pacyfiku. Jej główne aktywności koncentrują się na usługach IT, sieciowych usługach telekomunikacyjnych (lokalnych, krajowych i międzynarodowych) oraz usługach internetowych.

BT posiada trzy działy biznesowe:

- ✔ **BT Retail** – wszechstronny zakres usług komunikacyjnych dla ponad 20 milionów klientów indywidualnych i przedsiębiorstw w Wielkiej Brytanii,
- ✔ **BT Wholesale** – rozwiązania i usługi sieciowe dla ponad 600 operatorów telefonii stacjonarnej i komórkowej oraz dostawców usług internetowych,
- ✔ **BT Global Services** – rozwiązania IT i sieciowe na skalę globalną, pozwalające sprostać potrzebom organizacji prowadzących działalność w wielu stronach świata. BT Global Services prowadzi działalność w ponad 130 krajach.

Opracowano na podstawie materiałów firmy BT

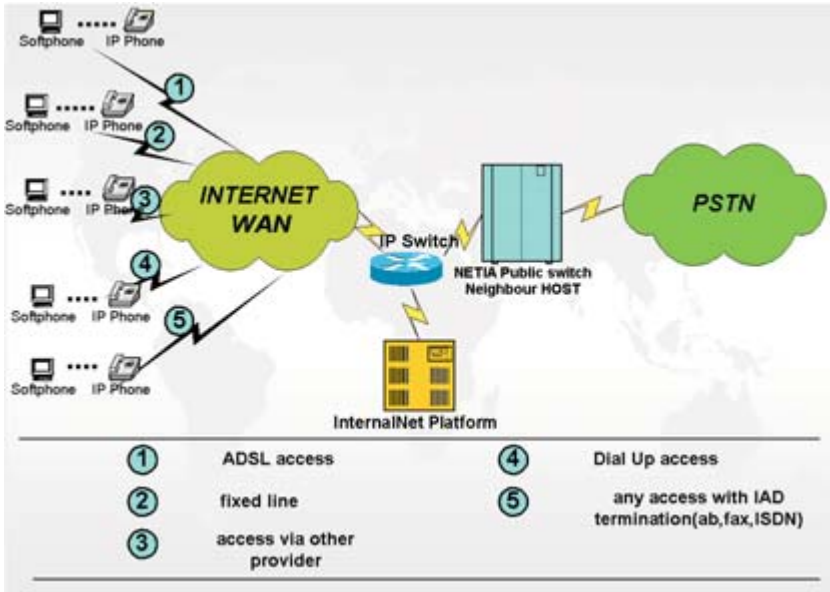
Netia – zintegrowane usługi dla biznesu w sieci operatora telekomunikacyjnego

IntegralNet to rozwiązanie bazujące na platformie integrującej usługi telekomunikacyjne operatora ze specyficznymi rozwiązaniami dla nowoczesnych central abonenckich (PABX). Model świadczenia usług opiera się na dostarczeniu przez operatora nie tylko usług głosowych i transmisji danych, ale również pełnej funkcjonalności wirtualnej centrali abonenckiej.

Rozwiązanie IntegralNet bazuje na obsłudze użytkowników, którzy mają dostęp do internetu. W IntegralNet użytkownicy telefonów oraz subskrypcja nowych abonentów nie są, jak do tej pory, przypisane do jednego miejsca geograficznego. Wykorzystując protokół IP oraz dostęp do internetu, w każdym miejscu pracownik firmy może korzystać z zasobów IntegralNet. Platforma oferuje szereg nowych funkcjonalności ułatwiających nie tylko zarządzanie własną częścią abonentów, ale również pozwala z nową jakością (Class 5 – określającą niezawodność urządzeń operatorskich) efektywnie zarządzać całą firmą. Wykorzystując obecny dostęp lub zestawiając nowe łącza do internetu klient może stać się abonentem usługi IntegralNet. Terminale abonenckie w postaci Net phone lub adapterów ab (IAD) są podłączane w wewnętrznej sieci LAN klienta. Liczba podłączonych terminali mających status użytkownika IntegralNet zależy od wykupionego pakietu zawierającego liczbę numerów telefonicznych zgodnych z krajowym planem numeracyjnym. Każdy numer-abonent IntegralNet posiada funkcjonalność klasycznego użytkownika korzystającego z funkcji central abonenckich PABX, a dzięki platformie IntegralNet funkcje te są mu oferowane przez internet.

Modele realizacji usług IntegralNet w Netii

Najważniejsza funkcjonalność to oczywiście realizowanie połączenia telefonicznego. Użytkownik strefy IntegralNet może skorzystać z wielu typów terminali np. Net phone, standardowy aparat analogowy, może również wysłać faks. Poprzez wybranie numeru wewnętrznego łączymy się z abonentem wydzielonej strefy IntegralNet w ramach jednej firmy.



Rys. 1. Schemat poglądowy sieci z IntegralNet

Administrator wirtualnej centrali IntegralNet może w bardzo łatwy sposób modelować łączność w swojej firmie przez interfejs web. Na przykład:

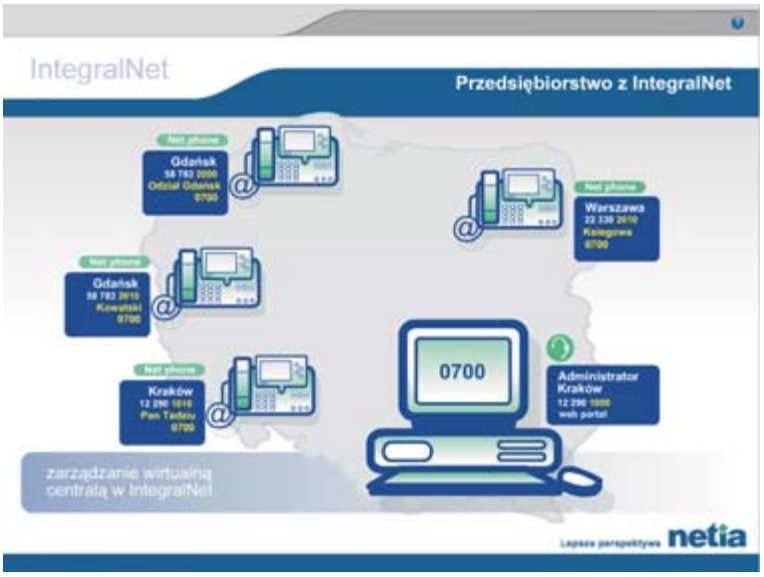
- ✔ nadawać nazwy abonentom,
- ✔ zabraniać wybierania określonych numerów,
- ✔ aktywować nowe usługi dla numerów wewnętrznych, np. pocztę głosową.

Użytkownik IntegralNet realizuje obecnie wiele funkcji dostępnych dotychczas z kosztownych aparatów systemowych poprzez aplikacje CTI powiązane z jego aparatem telefonicznym. Poprzez przeglądarkę internetową można w pro-

sty i szybki sposób korzystać z zasobów firmy (np. systemowa książka telefoniczna). Messaging – integracja poczty elektronicznej i wykorzystanie kontaktów z własnej książki adresowej – pozwala na pełny, niczym nieograniczony dostęp do informacji.

Oprócz szeregu funkcji administracyjnych jest też wiele korzyści, które pozwalają obniżyć koszty związane z łącznością w przedsiębiorstwie. Cały ruch telefoniczny zamykający się w ramach numerów wewnętrznych platformy IntegralNet jest wliczony w cenę abonamentu za usługę. Może to dotyczyć nie tylko jednego przedsiębiorstwa, ale również kilku współpracujących ze sobą kooperantów, tworzących na platformie IntegralNet grupę biznesową. Bardzo istotnym elementem jest również minimum inwestycji w infrastrukturę telekomunikacyjną w nowej siedzibie firmy lub brak konieczności zakupu nowej centrali PABX w przypadku potrzeby wymiany istniejącej. Wszystkie koszty utrzymania i zarządzania dotychczas używanymi centralami abonenckimi w przypadku zastosowania rozwiązania IntegralNet sprowadzają się do miesięcznego abonamentu. Ważną rolę odgrywa również kontrola kosztów połączeń telefonicznych wychodzących poza platformę IntegralNet. Pełną informację o tym ruchu telefonicznym, a co najważniejsze – możliwość szybkiego reagowania na ewentualne nadużycia posiada administrator IntegralNet.

Rys. 2. Dostęp usług głosowych na terenie całego kraju



Rys. 3. Administrowanie zasobami wirtualnej centrali

Co dalej

IntegralNet jest pierwszą usługą w ofercie Netii realizowaną w ramach sieci NGN (*Next Generation Network*). Głównym założeniem NGN jest dostarczanie wszelkiego typu usług i wartości (*content*), bez przypisywania i podziału na rodzaj dostępu do sieci użytku publicznego. Już niedługo podstawowym elementem konkurencyjności na rynku telekomunikacyjnym będzie lista usług dodanych (VAS – *value added services*), które staną się podstawowymi cechami wyróżniającymi poszukiwane przez klienta rozwiązanie. Dostęp do użytkownika IntegralNet przez jeden numer telefonu – niezależnie gdzie się znajduje, w domu, pracy, hotelu – jest tylko przykładem zastosowania integracji dostępnych zasobów w celu unifikacji i łatwości w komunikowaniu. IntegralNet jest platformą otwartą, umożliwiającą w przyszłości implementację i integrację różnego typu usług, funkcji i mediów dostępowych, np. GSM i UMTS.

Krzysztof Baryłowski
kierownik Działu Produktów Telefonii Korporacyjnej
Departament Zarządzania i Rozwoju Produktów
Netia SA

Produkt dla klienta – nigdy odwrotnie

Ważne jest nie tylko to, co się robi, ale również w jaki sposób. By efektywnie wprowadzić usługi szerokopasmowe i telefonię trzeciej generacji (3G), nie wystarczy sama oferta. Operatorzy będą musieli coraz lepiej poznawać klientów i skutecznie kształtować ich postawy.

Jeszcze nie tak dawno przetrwanie firmy na rynku telekomunikacyjnym zależało tylko od dobrej kontroli kosztów. I chociaż do dziś niewiele się pod tym względem zmieniło, najwięksi gracze są świadomi, że zwiększanie zysków nie jest możliwe bez wprowadzania nowych, innowacyjnych usług, wzmacniających więź między operatorem a klientem. Wiele firm dostrzega taką właśnie szansę w usługach szerokopasmowych i telefonii trzeciej generacji (3G).

– *Otwierają się nowe możliwości, widać cały wachlarz nowych zastosowań* – twierdzi Julian Hewett, analityk z brytyjskiej firmy konsultingowej Ovum. – *Przez branżę pędzi potężna fala zmian.*

Od zeszłego roku abonenci Orange we Francji mogą korzystać ze sterowanej głosem poczty głosowej. Operator nie twierdzi, że odkrył coś nowego. Siłę oddziaływania oferty przypisuje odwołaniu do najbardziej naturalnych ludzkich zachowań.

– *Używanie głosu to coś naturalnego dla każdego z nas przynajmniej od momentu, kiedy kończymy pierwszy rok życia* – mówi Rich Miner, wiceprezes Advanced Service Development Orange. – *Wystarczy wydać taki czy inny dźwięk i zaraz ktoś przybiegnie, by zaspokoić nasze potrzeby. To przecież nic innego, jak głosowy „dostęp do usług". Wyobraźcie sobie, że zamiast tego każemy dziecku przyciskać jakieś guziki!*

Abonenci Orange najwyraźniej zgadzają się z tym poglądem. Już w końcu 2004 roku z nowej usługi korzystało 4 miliony klientów. Z punktu widzenia Minera, to dopiero początek. Wraz z wprowadzeniem przekazu szerokopasmowego i telefonii 3G sytuacja stanie się o wiele bardziej interesująca.

– *Telefonia 3G jest jak widowisko z gatunku „światło i dźwięk"* – twierdzi. – *Głos i obraz są ze sobą powiązane, tworzą nową wartość. Żeby dowiedzieć się, jaka będzie pogoda, użyjemy głosu. Odpowiedzią będzie obraz pokazujący prognozę na przykład w formie ikon.*

Wiele firm widzi w nowych usługach klucz do stworzenia jeszcze silniejszej więzi między operatorem a klientem.

– *Operatorzy są dziś świadomi, że najcenniejsze zasoby firmy to... klienci* – mówi Glenn James, prezes Unisys Global Communications and Media Practice. – *A to oznacza, że proponowanie nowych usług, które zaspokoją specyficzne oczekiwania klientów, jest równoznaczne z zadowoleniem udziałowców.*

Jednak nowe usługi, jak każde inne *novum*, mogą okazać się mieczem obosiecznym – przestrzegają eksperci. Chociaż ich wprowadzenie niesie z sobą obietnicę zwiększenia lojalności klientów, potencjalnie mogą przynieść całkiem odwrotne skutki. Stanie się tak, jeśli nowe techniki okażą się dla klientów zbyt skomplikowane albo po prostu niepotrzebne. Sukces operatora nie zależy tylko od tego, co nowego zaproponuje abonentom. Nie mniej ważny jest również sposób, w jaki się do tego zabierze.

Rozwój dzień po dniu

Zmierzając w kierunku usług szerokopasmowych i telefonii 3G firmy skupiały się przede wszystkim na inwestycjach w infrastrukturę. Zdaniem Hewetta, nadszedł czas, by zdecydować, które usługi wprowadzić. Wachlarz możliwości jest bardzo szeroki, począwszy od udostępniania serwisów informacyj-

nych aż po – wykorzystywany do różnych celów – przekaz wizualny.

– Nie możemy zapominać, że istnieje podstawowa różnica między klientami usług szerokopasmowych i tymi, którzy korzystają z łączności bezprzewodowej – podkreśla Hewett. *– Dla tych pierwszych ilość pobieranych danych nie ma większego znaczenia, dla drugich, wręcz przeciwnie. Podczas gdy pierwsi będą zainteresowani na przykład filmami, drudzy będą wymagać przede wszystkim „lekkich" danych.*

– Przekaz szerokopasmowy i telefonia 3G kusi, by stworzyć zintegrowaną ofertę, dać zarówno użytkownikom indywidualnym, jak i biznesowym „pełnię szczęścia": ciągły i jednoczesny dostęp do wszystkich kanałów komunikacyjnych, telefonu, poczty elektronicznej, przekazu wideo i internetu. W takim środowisku – twierdzi Hewett – *nie sposób przecenić znaczenia nowych modeli biznesowych. Więksi dostawcy mogą dostrzec konkretną wartość we współpracy z mniejszymi firmami, dostarczającymi zawartość przeznaczoną wyłącznie dla specyficznego odbiorcy, taką, którą duża firma z przyczyn czysto ekonomicznych nie może się poważnie zainteresować.*

– Musimy przemyśleć jeszcze wiele istotnych kwestii – podkreśla Hewett. *– Mamy przed sobą równanie z ogromną liczbą niewiadomych i nie sądzę, by ktokolwiek dziś był w stanie przewidzieć, jakie konsekwencje spowoduje pojawienie się usług szerokopasmowych i telefonii trzeciej generacji. Nie wiadomo, za co ludzie będą skłonni zapłacić. Wchodzimy na zupełnie nieznany teren.*

Jednym z najważniejszych tematów do przemyślenia pozostaje wciąż kwestia podstawowego – jeśli chodzi o zyski – zastosowania nowych możliwości.

– Jeżeli takie zastosowanie w ogóle istnieje – dodaje Nick Lake, dyrektor Market Source Consulting Unisys. *– Wątpię, by w przypadku szerokopasmowego dostępu i telefonii 3G można było spodziewać się produktów, które podbiją masowy rynek i staną się podstawowym źródłem przychodów. Widziałbym raczej w tej roli wiele różnych zastosowań niszowych.*

W takich warunkach innowacyjność i nieustanne wzbogacanie oferty okaże się z pewnością krytyczne. Przyjęcie takiego założenia powoduje daleko idące konsekwencje.

– Nie można stawiać wszystkiego na jedną kartę, szczególnie na rynku, na którym nic nie jest pewne: ani to, czego oczekują klienci, ani przebieg wydarzeń, ani skuteczność działań, ani też, co takiego może przemówić ludziom do wyobraźni – twierdzi Miner. *– Realizowanie obliczonych na wiele lat planów rozwoju usług i produktów wydaje się w tym przypadku mniej ryzykowne niż jednoczesne inwestowanie w różnych obszarach.*

Podobnie widzi tę kwestię Hewett. *– Rozwój zmusza firmy do ciągłego prowadzenia eksperymentów. Wygrywa ten, kto potrafi przeprowadzić je taniej i szybciej... i ma dobre wyczucie rynku.*

Całościowe spojrzenie

Rozwój to wspaniała perspektywa. Firmy powinny jednak uważać, by przez przypadek nie zostawić klientów w tyle.

– Rozwój technologiczny zawsze prześciga potrzeby i oczekiwania klientów – mówi Lake. *– Sztuka polega na tym, by łagodzić ten efekt, rozwijać się w odpowiednim tempie; upewniać się, że „odległość"*

między nowymi produktami i usługami a możliwościami ich wykorzystania przez klientów nie rośnie.

Operatorzy telekomunikacyjni będą musieli aktywnie kształtować postawy klientów, a to oznacza coś więcej niż tylko przedłożenie nowej oferty. Muszą potraktować problem całościowo, uwzględnić wszystkie płaszczyzny funkcjonowania przedsiębiorstwa: strategię i technologię, przebieg procesów biznesowych i marketing. Konieczne okaże się również budowanie relacji partnerskich z innymi firmami. A co najważniejsze, trzeba będzie zwrócić większą uwagę... na samych klientów.

– Żeby skutecznie budować lojalność w przypadku szerokopasmowego dostępu i 3G, firmy będą musiały położyć większy nacisk na edukację użytkowników – twierdzi Lake. *– Centra obsługi telefonicznej, rozbudowane strony internetowe, indywidualna pomoc w punktach sprzedaży staną się podstawowymi narzędziami. Skierowany do klienta przekaz musi być jasny, prosty i jednoznaczny.*

Zdaniem Lake'a, oswajanie klientów z nowymi usługami musi przebiegać stopniowo. Być może rozwiązaniem okaże się wprowadzenie ofert przewidujących, iż klient będzie mógł przez pewien czas korzystać z nich za darmo, podobnie jak ma to miejsce w przypadku wersji *trial* oprogramowania. Można także wyobrazić sobie inne wersje przebiegu wydarzeń. Lake powołuje się tu na koncepcję jednego z operatorów, który wprowadzając wraz z ofertą 3G wizualną pocztę głosową jednocześnie umożliwił posiadaczom tradycyjnych telefonów korzystanie z niej za pośrednictwem internetu.

– Jest to głęboko przemyślane posunięcie – twierdzi Lake. *– Wprowadzając ofertę 3G firma tworzy, by tak rzec, „usługi przejściowe", dokłada starań, by właściciele zwykłych telefonów nie czuli się wyrzuceni poza nawias. Oni również w pewnym stopniu mogą korzystać z rozwoju technologii.*

Podobnemu celowi służy, zdaniem Minera, opierająca się na platformie Unisys, sterowana głosem poczta głosowa Orange.

– Nowa usługa spełnia w tej chwili funkcję edukacyjną – podkreśla Miner. *– Uczymy 4 miliony ludzi, jak korzystać z usług kierowanych głosem. Oferta takich usług będzie się systematycznie zwiększać.*

Pytanie „co" i pytanie „jak"

Tak czy inaczej, utrzymanie lojalności dotychczasowych klientów będzie wymagać od operatorów wiele wysiłku. Muszą dokładnie zrozumieć motywacje użytkowników, co oznacza konieczność zmiany nastawienia. Znajdujący się dotychczas w centrum zainteresowania firm produkt musi ustąpić miejsca klientowi, a tradycyjna segmentacja klientów (np. pod względem wieku) – podziałowi uwzględniającemu styl życia i kierującym zachowaniami emocjom.

– Firmy telekomunikacyjne powinny dokładnie poznać i uwzględnić wpływ, jaki rozwój technologiczny wywiera na psychikę klientów – twierdzi Lake. *– Jak zmienia ich samoocenę i własny image, który pragnęliby narzucić innym. Tylko zrozumienie aspiracji pozwoli przewidzieć ich zachowania w przyszłości.*

– Lojalności klientów nie traci się dając im więcej, niż potrzebują – mówi Miner. *– Z całą pewnością odejdą, jeśli poczują się sfrustrowani. Nie chodzi więc tylko o to, by oferować im nowe usługi. Trzeba jeszcze zaproponować je w taki sposób, by byli w stanie je zaakceptować i z nich korzystać.*

Przystosowanie firm telekomunikacyjnych do nowej sytuacji będzie wymagać zmian nastawienia na każdym poziomie ich aktywności. Muszą działać szybko i efektywnie, a jednocześnie – minimalnym kosztem. Przede wszystkim należy zwrócić uwagę na przepływ informacji dotyczących klientów – począwszy od gromadzenia danych, przez analizę, aż po wprowadzanie w życie płynących z tej analizy wniosków.

– Budowanie lojalności w dobie szybkich zmian technologicznych to nie tylko kwestia technologii i jej zastosowań – podkreśla Lake. *– To także kwestia doświadczeń i przyzwyczajeń klientów. Innymi słowy, pytaniu „co" musi w przypadku wprowadzania nowych usług towarzyszyć pytanie „jak".*

Peter Haapaniemi

Zagrożone sieci bezprzewodowe

Specjaliści ostrzegają, że szybki rozwój sieci bezprzewodowych w wielu miastach naraża firmy na ataki „podróżujących hakerów" oraz inne zagrożenia bezpieczeństwa. Badania zlecone przez RSA Security wykazały, że ponad jedna trzecia firm używających sieci bezprzewodowych jest podatna na ataki z ulicy lub sąsiednich budynków.

– Dla potencjalnego hakera to prawie jak spacer wzdłuż ulicy i naciskanie klamek kolejnych drzwi, jest niemal pewne, że któreś się otworzą – mówi **Tim Pickard**, wiceprezes regionu ds. międzynarodowego marketingu (*Area VP of International Marketing*) w RSA Security. *– Nasze badania wykazały, że w samych tylko europejskich centrach finansowych sieci bezprzewodowe rozrastają się w tempie co najmniej 66 proc. rocznie, a ponad jedna trzecia firm nie ma zabezpieczeń przed atakami z tego kierunku.*

Badania prowadzono w centrach biznesu we Frankfurcie, Londynie, Nowym Jorku i San Francisco. We wszystkich tych miastach ponad jedna trzecia firmowych sieci bezprzewodowych nie jest bezpieczna, dotyczy to 36 proc. firm w Londynie, 34 proc. we Frankfurcie, 38 proc. w Nowym Jorku i 35 proc. w San Francisco.

Ponadto, okazało się, że wiele firm nie stosuje nawet podstawowych środków bezpieczeństwa, takich jak zmiana domyślnej konfiguracji sieci. Oznacza to, że wiele punktów dostępowych sieci bezprzewodowych może wysyłać informacje ułatwiające atak potencjalnym hakerom. Ustawienia domyślne ma 26 proc. punktów dostępowych w Londynie, 30 proc. we Frankfurcie, 31 proc. w Nowym Jorku i 28 proc. w San Francisco.

Oprócz zagrożeń bezpieczeństwa występujących w firmach badania wykazały szybki wzrost liczby publicznych punktów dostępowych. Należy do nich 12 proc. wszystkich bezprzewodowych punktów dostępowych w Londynie, 24 proc. we Frankfurcie, 21 proc. w Nowym Jorku i 12 proc. w San Francisco.

– Liczby te są dla wszystkich niezabezpieczonych firm kolejnym poważnym ostrzeżeniem, które powinno skłonić je do szybkiego działania – twierdzi **Phil Cracknell**, dyrektor ds. technicznych w firmie netSurity i autor raportu. *– Szybki wzrost liczby publicznych bezprzewodowych punktów dostępowych następuje równolegle ze wzrostem zagrożeń dla firm, które używają sieci bezprzewodowych o słabych zabezpieczeniach lub w ogóle bez nich. Możliwość przypadkowego lub zamierzonego połączenia się z siecią korporacyjną naraża firmę na różne niebezpieczeństwa, na przykład utratę poufnych danych lub zainstalowanie szkodliwego programu. Możliwość korzystania z bardzo rozpowszechnionych publicznych punktów dostępowych sprawia, że użytkownicy mobilni będą coraz częściej wykorzystywać sieci bezprzewodowe. Pytanie tylko, do czyjej sieci się dostaną oraz co zrobią, kiedy już do niej wejdą.*

Tim Pickard z RSA Security dodaje: *– Wyniki te wyjaśniają, dlaczego tak ważne jest zwiększenie w firmach świadomości zagrożeń występujących w sieciach przewodowych i bezprzewodowych. Badania są prowadzone już czwarty rok i nie ma żadnych oznak poprawy sytuacji. Korzyści, jakie zapewnia elastyczna i łatwa w użyciu technologia bezprzewodowa, są oczywiste, ale należy również stosować odpowiednie zabezpieczenia.*

Posługując się laptopem i oprogramowaniem dostępnym bezpłatnie w internecie specjaliści prowadzący badania mogli przechwytywać informacje z korporacyjnych sieci bezprzewodowych po prostu jeżdżąc samochodem ulicami miast. Tak łatwy dostęp niepowołanych osób do sieci korporacyjnej może być wykorzystany do uzyskania poufnych informacji, zakłócenia działalności przedsiębiorstwa lub przeprowadzenia ataku przez internet na inną firmę.

Badania zostały wykonane na zlecenie RSA Security, firmy zajmującej się ochroną tożsamości i dostępu do informacji. Przeprowadziła je niezależna firma netSurity specjalizująca się w problematyce bezpieczeństwa informacji. Badana służyły ocenie skali „wycieków" danych z korporacyjnych sieci bezprzewodowych dających hakerom możliwość dostępu do informacji z samochodów lub sąsiednich budynków.

Opracowano na podstawie materiałów firmy RSA Security

Fot. Alcatel

Od dostawcy do integratora usług teleinformatycznych

Sieć teleinformatyczna jest wykorzystywana przez firmy w coraz szerszym zakresie, nie tylko do dostępu do internetu, intranetu i poczty elektronicznej, ale także do pełnego dostępu do zasobów korporacyjnych WWW czy obsługi wybranego systemu transakcyjnego. Dzięki sieciom możliwe jest połączenie rozproszonych geograficznie placówek działających w ramach jednej korporacji, co z kolei umożliwia bezpośrednią transmisję danych i głosu. Na rynku wzrasta popularność wykorzystania złożonych sieci teleinformatycznych, a także zwiększa się zakres usług, jakie firma decyduje się powierzyć dostawcy.

Odbiorcy usług ITC coraz częściej zamawiają nie tylko sprzęt konieczny do technicznego zestawienia połączeń, ale także decydują się na pełen outsourcing usług związanych z zarządzaniem, utrzymaniem, konserwacją i naprawami sieci, jednocześnie korzystając z szerszego pakietu usług dodatkowych. Ewolucję potrzeb zgłaszanych przez klientów operatorów telekomunikacyjnych ilustrują poniższe opisy doświadczeń i wdrożeń Crowley Data Poland.

Krok pierwszy: Dzierżawa łączy Frame Relay

Podstawowy zakres usług, czyli dostarczenie klientowi sieci korporacyjnej, ilustruje przykład zamówienia złożonego przez Telewizję Polską na przełomie 2002 i 2003 roku. Na życzenie klienta, Crowley Data Poland połączył jedenaście oddziałów regionalnych TVP z siedzibą główną w Warszawie przy ulicy Woronicza 17. Projekt opierał się głównie na dzierżawie łączy Frame Relay – protokołu transmisji danych stosowanego na rozległych sieciach komputerowych. Rozwiązanie to umożliwiło odbiorcy szybką – z przepustowością do 2 Mbit/s – transmisję danych pomiędzy lokalizacjami. Zakres projektu obejmował centralny dostęp do internetu, który w kolejnym roku świadczenia usługi rozszerzony został do przepływności 20 Mbit/s z możliwością rozszerzenia do 40 Mbit/s. Klient odpowiedzialny był za konfigurację własnych urządzeń aktywnych oraz za zarządzanie całą siecią. Do konfiguracji usługi wykorzystano sieć dostępową Crowley oraz sieć czterech innych operatorów. Przedsięwzięcie zrealizowano za pomocą światłowodów, łączy radiowych oraz łączy miedzianych.

Krok drugi: Dzierżawa podstawowych i zapasowych łączy telekomunikacyjnych, instalacja i konfiguracja urządzeń, dostęp do internetu

Projekt zrealizowany na potrzeby dużej firmy z branży produkcyjnej opierał się na dostawie łączy transmisji danych o przepływności 512 kbit/s – 2 Mbit/KB. Było to połączenie o gwarantowanej przepływności, zachowujące najwyższe parametry bezpieczeństwa transferu danych. Usługa pozwoliła na elastyczną konfigurację

Sieć korporacyjna Telewizji Polskiej SA

łącza transmisyjnego poprzez indywidualny dobór odpowiedniej szybkości gwarantowanej. W projekcie wykorzystano łącza zapasowe oparte na technologii ISDN, gwarantujące niskie koszty utrzymania sieci zapasowej. Ponadto w tej realizacji zastosowano zarówno łącza radiowe, jak i łącza miedziane. Rozwiązanie umożliwiło połączenie wielu sieci komputerowych dedykowanymi łączami o indywidualnie dobranych parametrach. Konfiguracja połączenia każdej lokalizacji była realizowana oddzielnie, w zależności od faktycznych potrzeb. Rozwiązanie to zawierało więcej elementów niż w przypadku Telewizji Polskiej: Crowley dostarczył również kompleksową usługę instalacji i konfiguracji urządzeń aktywnych (routerów i firewalli), łączy zapasowych oraz monitoring całego rozwiązania.. Zarządzanie siecią pozostało po stronie klienta.

Krok trzeci: Outsourcing telekomunikacyjny

Jednym z najbardziej złożonych projektów zrealizowanych w roku 2004 przez Crowley Data Poland był outsourcing telekomunikacyjny zaproponowany Najwyższej Izbie Kontroli. Projekt dotyczył budowy rozległej sieci WAN, dzięki certyfikatowi jakości usługi (SLA) zagwarantowano odpowiedni poziom świadczenia transmisji danych i szybki czas reakcji na ewentualne awarie. Crowley dostarczył urządzenia i rozwiązania w technologii Frame Relay oraz sieć zapasową zrealizowaną w oparciu o łącza ISDN do 17 lokalizacji NIK-u w całej Polsce. Elementem projektu była również dostawa, instalacja, konfiguracja i utrzymanie urządzeń abonenckich (routerów i firewalli) oraz przeprowadzenie szkoleń dotyczących wdrażanej usługi i technologii telekomunikacyjnych dla pracowników NIK. Klient zlecił operatorowi wszelkie zadania związane z zarządzaniem siecią. W przypadku tego projektu wykorzystano sieć Crowley oraz sieci dwóch innych operatorów oraz zastosowano łącza radiowe i łącza miedziane, a także dwuwarstwowy model koncepcyjny (OSI). W roku 2005 projekt zostanie poszerzony o transmisję głosu przy wykorzystaniu technologii VoIP.

W sektorze dużych korporacji oraz średnich i małych przedsiębiorstw zmiany oferty operatorów dotyczą jej zakresu – pakiet usług świadczonych przez dostawców staje się coraz szerszy i bardziej kompleksowy. Do usług transmisji danych dołączane są usługi głosowe, dostawy, instalacje i zarządzanie sprzętem, zarządzanie siecią oraz cały szereg usług dodanych, takich jak łącza zapasowe (*backupowe*), zdalny dostęp, kolokacja czy zarządzanie bezpieczeństwem. Działalność polegająca na świadczeniu wielu usług w postaci opisanej powyżej bywa nazywana integracją telekomunikacyjną lub outsourcingiem telekomunikacyjnym.

Można przypuszczać, że integracja usług telekomunikacyjnych będzie postępować i operatorzy będą coraz chętniej oferować usługi zintegrowane. Wynika to z faktu, że oferując jednocześnie usługi transmisji danych i głosu, uzupełnione o inne usługi dodane, operator jest w stanie z jednej strony wykazać istotne oszczędności u klienta (np. polegające na obniżeniu kosztów utrzymania infrastruktury głosowej), a z drugiej – zachęcić szerokim portfelem usług do bliższego zapoznania się z jego ofertą. Tendencja ta nasila się w ostatnim czasie i coraz częściej skłania operatorów telekomunikacyjnych do współpracy z integratorami systemowymi. Dzięki temu zarówno operatorzy, jak i integratorzy są w stanie zaspokoić wszelkie potrzeby klienta związane z teleinformatyką, a odbiorca zyskuje kompleksową i dopasowaną do jego potrzeb ofertę.

Robert Idziak
dyrektor Działu Rozwiązań i Produktów
Crowley Data Poland

Sieć korporacyjna Najwyższej Izby Kontroli

Optymalizacja korporacyjnych struktur sieciowych, czyli światłowodem do biura

Nowoczesna komunikacja i stale rosnące zapotrzebowanie na szybką transmisję danych wymagają perspektywicznie zorientowanych koncepcji sieciowych. Współczesne tendencje wskazują na światłowód, jako na medium będące podstawą teletransmisyjnej sieci przyszłości.

W krajach Europy Środkowowschodniej z roku na rok przybywa instalacji światłowodowych w sieciach korporacyjnych. Jednak daleko nam jeszcze do zachodnich sąsiadów zarówno pod względem ilości, jak i skali przeprowadzanych inwestycji.

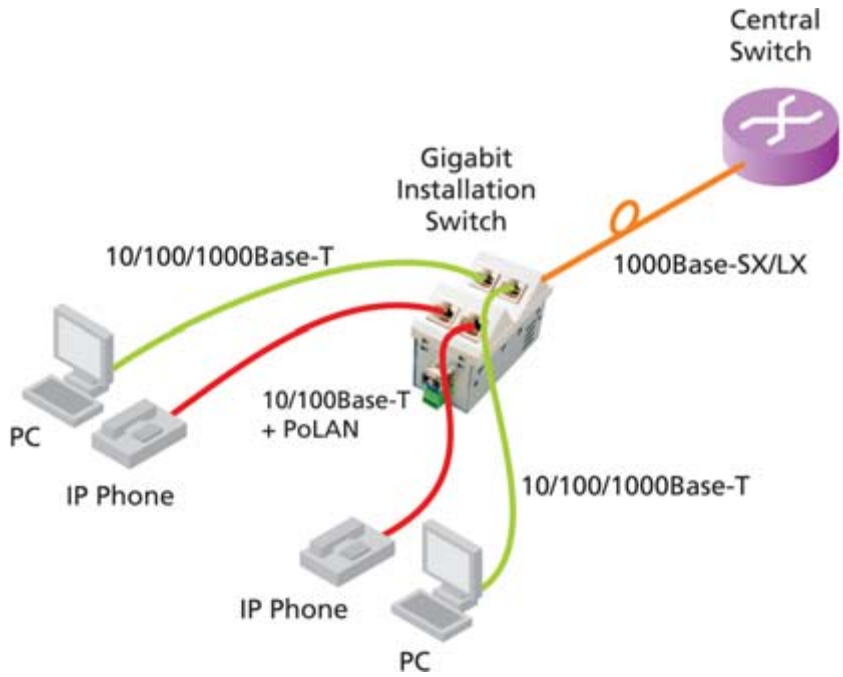
Wykorzystując amerykańską koncepcję okablowania bazującą wyłącznie na nieekranowanej skrętce zapominamy często o aplikacjach optycznych z ich niekwestionowanymi zaletami i związanymi z nimi znaczącymi oszczędnościami.

Opis koncepcji FTTO (Fiber to the Office)

Wykorzystując właściwości światłowodu umożliwiające transmisję danych na duże odległości można scentralizować dystrybucję sieciową w jednym punkcie. Taka koncepcja określana jest mianem *collapsed backbone*. Dzięki zastosowaniu takiego rozwiązania nie ma już konieczności zajmowania kolejnych pomieszczeń na kosztowne centra subdystrybucyjne wraz z dodatkowym wyposażeniem.

Zastosowanie konwerterów wieloportowych w centrum dystrybucyjnym pozwala na ekonomiczną konwersję portów miedzianych na światłowodowe. Dzięki temu

Switch instalacyjny Gigabit, wersja z portem uplink SFP



24-portowy zarządzalny konwerter 100BaseTX/100BaseFX

można wykorzystać aktywne urządzenia wyposażone w porty miedziane, co w znacznym stopniu obniża koszty sieci.

Chcąc doprowadzić światłowód do biura można wybierać spośród szerokiego asortymentu przełączników (wolno stojących, przystosowanych do montażu w naściennych kanałach kablowych lub podłogowych puszkach dystrybucyjnych) konwertujących każdy port centralnego przełącznika na cztery porty terminali. Wszystkie urządzenia końcowe mogą być podłączone do sieci poprzez standardowy kabel miedziany, a chcąc unowocześnić sieć, należy wymienić tylko urządzenia końcowe.

Urządzenia

Wieloportowe konwertery mediów mają postać kompaktowych urządzeń Ethernet lub Fast Ethernet o dużej gęstości portów. Możliwe jest zabudowanie 24 par portów (skrętka + światłowód) w urządzeniu o wysokości 1U. Przy Gigabit Ethernet w urządzeniu o wysokości 3U można zrealizować konwersję do 18 portów. Oprócz wysokiego zagęszczenia portów systemy konwersji wyposażone są w redundantne zasilanie, funkcję autocrossing oraz zarządzanie SNMP/web based. Maksymalny zasięg transmisji światłowodowej w trybie full duplex dla włókien wielomodowych to: 2 km dla Fast Ethernet oraz 275/550 m dla Gigabit Ethernet. Przy włóknach jednomodowych zasięg dla obydwu protokołów wynosi 15/30/80/125 km w zależności od wersji interfejsu optycznego. Przy zastosowaniu systemu modularnego istnieje możliwość konwersji różnych protokołów w jednym chassis.

Urządzenia końcowe – switche wolno stojące, montowane w kanałach instalacyjnych lub podpodłogowych – są technologicznie zaawansowanymi przełącznikami warstwy drugiej z zaimplementowanymi mechanizmami nadawania priorytetów z warstwy trzeciej oraz CoS dla aplikacji VoIP, z obsługą sieci VLAN zgodnie z IEEE 802.1pq. Switche wspierają również zasilanie urządzeń końcowych przez skrętkę PoE (*Power over Ethernet*) zgodnie z IEEE 802.1af. Oprócz interfejsu światłowodowego Fast Ethernet posiadają w zależności od wersji 4 lub 6 portów skrętkowych. Zasięg transmisji poszczególnych protokołów jest analogiczny jak w przypadku konwerterów wieloportowych i modularnych. W wersji miniaturowej 45x45 mm do montażu w kanałach kablowych i podpodłogowych przełączniki można wyposażyć w uplink światłowodowy Gigabit Ethernet mający postać portu optycznego zabudowanego na stałe lub modularnego jako transceiver SFP. Komunikacja z urządzeniami odbywa się przez SNMP, TCP/IP lub Telnet. Dodatkowo oferowane jest oprogramowanie Device Manager, umożliwiające administrowanie dużymi sieciami FTTO w efektywny sposób. Ze względów bezpieczeństwa może zostać wdrożone opcjonalne oprogramowanie do identyfikacji MAC, które uniemożliwia dostęp do centralnych zasobów nieuprawnionym użytkownikom.

Urządzenia dedykowane do realizacji koncepcji FTTO umożliwiają realizację całości okablowania przy pomocy światłowodu, a zarazem podłączenie końcowych urządzeń za pośrednictwem kabla miedzianego. Stanowią tym samym ekonomiczne i przyszłościowe rozwiązanie inwestycyjne.

Switch instalacyjny MICROSENS z funkcjonalnością PoLAN współpracujący z telefonem IP

Podstawowe atuty rozwiązań FTTO:

- ✔ pionowe i poziome okablowanie światłowodowe budynku,
- ✔ elastyczność i skalowalność sieci,
- ✔ bezpieczeństwo transmisji, brak zakłóceń, izolacja galwaniczna,
- ✔ brak kosztownych centrów subdystrybucyjnych,
- ✔ pokonanie bariery 90 m na skrętce,
- ✔ beznarzędziowy montaż *snap-in* urządzeń instalacyjnych,
- ✔ kompatybilność urządzeń instalacyjnych z systemem Mosaic m.in. Legrand, Ackermann,
- ✔ integracja z telefonią IP,
- ✔ efektywna administracja.

Marcin Dąbrowski
Account Manager w firmie Microsens (www.microsens.com)

Jak zabezpieczyć sieć

Doświadczenia ostatnich kilku lat pokazują jednoznacznie, iż bezpieczeństwo sieci i narzędzia służące do jego tworzenia będą w nadchodzącym okresie czynnikiem krytycznym dla utrzymania i kontroli własnych systemów informatycznych. Warto zwrócić uwagę na fakt, że zagrożenia dla systemów i urządzeń pojawiające się po roku 2000 charakteryzują się całkiem inną postacią aniżeli zagrożenia, z którymi administratorzy borykali się kilka lat wcześniej. Ogromna część notyfikowanych ataków to robaki i wirusy, które rozprzestrzeniają się z niespotykaną dotąd szybkością i dokonują spustoszeń w systemach produkcyjnych na skalę nienotowaną przed rokiem 2000.

Jak bronić się przed nowymi zagrożeniami? Oczywiście, można stosować narzędzia reaktywne, jednakże ich skuteczność jest tak duża, jak szybkość reakcji ich producenta, który powinien jak najszybciej dostarczyć sygnaturę robaka lub wirusa. Opcja druga to zastosowanie innych metod pozwalających na kontrolę dostępu do sieci urządzeń, gdzie kryterium jest „dobra kondycja" hosta i niska podatność na zarażenie wirusem czy zainfekowanie robakiem internetowym. Jednym z rozwiązań, które umożliwia taką kontrolę dostępu, jest Network Admission Control (NAC).

Rozwiązanie Network Admission Control zakłada, iż nawet w przypadku prawidłowej, optymalnej konfiguracji sieci możliwe jest, iż w sieci będzie pojawiał się ruch niepożądany, w szczególności ruch generowany przez wirusy i internetowe robaki, który służy ich rozprzestrzenianiu się. Takie założenie wskazuje jednoznacznie, iż kontrola dostępu do sieci w oparciu o adresy MAC, adresy IP czy też port usługi nie jest wystarczająca dla zahamowania ataku wirusa czy robaka. Konieczne jest wprowadzenie dodatkowego elementu kontroli. Tym dodatkowym kryterium może być sprawdzenie, czy dany host żądający dostępu do sieci posiada zainstalowane i uruchomione odpowiednie aplikacje chroniące jego samego przez atakiem.

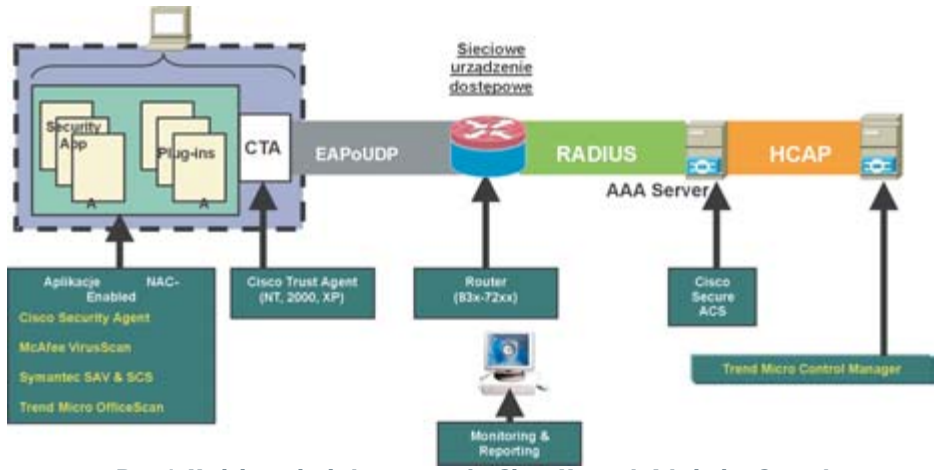
Elementami składowymi rozwiązania Cisco Network Admission Control są następujące komponenty:

- ✔ urządzenie sieciowe Cisco (router, a w przyszłości także przełącznik sieciowy, punkt dostępu bezprzewodowego, koncentrator VPN etc.) wraz z odpowiednim oprogramowaniem IOS,
- ✔ oprogramowanie komunikacyjne instalowane na stacjach roboczych – Cisco Trust Agent,
- ✔ serwer uwierzytelnienia i autoryzacji, podejmujący decyzję o dopuszczeniu użytkownika do sieci – Cisco Secure Access Control Server.

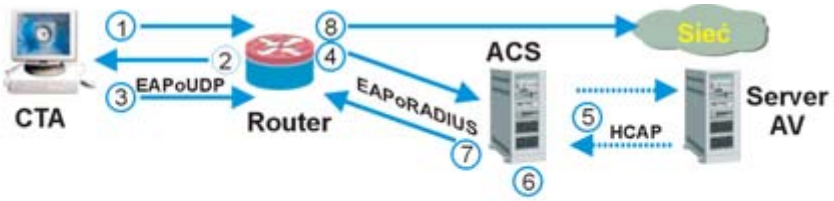
Model działania Network Admission Control

Czynnikiem warunkującym odporność systemu końcowego na zagrożenia z sieci LAN oraz z sieci zewnętrznych jest dedykowane oprogramowanie. Jest to w szczególności pakiet oprogramowania antywirusowego, oprogramowanie Host Intrusion Protection System (HIPS) zawierające Personal Firewalla etc. Trzeba pamiętać, żeby po instalacji tego oprogramowania odpowiednio je skonfigurować oraz często aktualizować. Spełnienie tych warunków jest konieczne, jeżeli użytkownik chce uzyskać dostęp do sieci. Rozwiązanie NAC współpracuje w tym zakresie z oprogramowaniem antywirusowym TrendMicro OfficeScan, Symantec SAV, McAfee VirusScan oraz z systemem HIPS – Cisco Security Agent.

O ile sprawdzenie czy też wymuszenie uruchomienia poszczególnych aplikacji jest stosunkowo proste, np. przez LoginScript, to już sam fakt wymiany informacji



Rys. 1. Umiejscowienie komponentów Cisco Network Admission Control



1. Użytkownik włącza komputer. Chce nawiązać komunikację do serwera. Pierwszy pakiet IP jest przechwytywany przez router i następuje uruchomienie procesu sprawdzania dla danego hosta.
2. Router uruchamia tzw. posture validation – proces odpytania CTA o kondycję bezpieczeństwa hosta – uruchomione aplikacje etc. Komunikacja odbywa się za pomocą EAPoUDP.
3. Po zebraniu informacji o uruchomionych aplikacjach CTA wysyła je (tzw. posture credentials) do routera – również z wykorzystaniem EAPoUDP.
4. Router wysyła otrzymane „posture credentials" do serwera CSACS – dla podjęcia decyzji o wpuszczeniu użytkownika do sieci lub też jego odrzuceniu. Komunikacja odbywa się przez EAPoRADIUS.
5. Gdy jest to potrzebne, serwer CSACS może działać jako proxy dla dodatkowego „posture validation" na serwerze AV. Dzieje się tak wówczas, gdy jednym z kryteriów składowych dopuszczenia do sieci jest element unikatowy dla danej aplikacji antywirusowej. Komunikacja pomiędzy serwerami ACS oraz AV jest szyfrowana i odbywa się za pomocą protokołu HCAP.
6. Serwer CSACS na podstawie danych otrzymanych z CTA oraz odpowiedzi otrzymanych z serwera ACS ocenia „kondycję hosta" („Zdrowy", „Do kwarantanny" etc.).
7. W przypadku gdy host jest dopuszczony do sieci lub warunkowo dopuszczony do sieci, serwer CSAC wysyła Access-Accept do routera z ograniczeniami (listy dostępowe) dla użytkownika.
8. Host otrzymuje/nie otrzymuje, otrzymuje z ograniczeniami dostęp do sieci IP.

Rys. 2. Schemat działania agenta CTA

z serwerem uwierzytelnienia i autoryzacji (Cisco Secure Access Control Server – CSACS) oraz cykliczne sprawdzanie kondycji hosta wymaga zastosowania dodatkowych narzędzi. W rozwiązaniu NAC taką funkcję pełni Cisco Trust Agent (CTA), który na żądanie urządzenia sieciowego sprawdza stan poszczególnych aplikacji oraz przesyła zebrane informacje do serwera CSACS. Agent CTA może pobierać informacje z innych aplikacji, zatem politykę dopuszczenia użytkownika do sieci można kreować bardzo elastycznie – zgodnie z wymaganiami i oczekiwaniami administratorów.

Informacje zebrane przez CTA są przesyłane do serwera CSACS przez urządzenia sieciowe w postaci zaszyfrowanej. Serwer CSACS podejmuje na bazie otrzymanych informacji decyzję, czy host z zabezpieczeniami w stanie takim, jak to zebrał agent CTA, może być dopuszczony do sieci.

Stan hosta jest cyklicznie sprawdzany, wykorzystuje się do tego celu mechanizm zapytań konfigurowanych na urządzeniach sieciowych. Pozwala to na płynne wykrywanie użytkowników, którzy z różnych powodów wyłączają poszczególne aplikacje zabezpieczające hosta. W przypadku zanotowania takiego faktu może zostać zablokowany dostęp użytkownika do sieci.

Mechanizm Network Admission Control pozornie nie wnosi wiele do istniejących systemów sieciowych i zabezpieczeń hostów. Warto jednak zauważyć kilka aspektów, które mogą okazać się krytyczne dla funkcjonowania infrastruktury informatycznej w organizacji, a które są adresowane przez mechanizmy NAC:

1. Użytkownik jest zobligowany do korzystania z aktualnych „engine" skanujących w oprogramowaniu antywirusowym i najnowszych plików z sygnaturami wirusów. Powoduje to automatyczne uwolnienie administratora od konieczności skrupulatnego wyłapywania użytkowników, którzy uruchamiają komputer bez dostępu do sieci po to, by po chwili dołączyć kabel – chcą uniknąć niedogodności związanych z aktualizacją zasobów.
2. Użytkownik jest zobligowany do korzystania z oprogramowania HIPS, co znacząco obniża prawdopodobieństwo zarażenia wirusem lub robakiem czy prawdopodobieństwo ataku na system operacyjny (np. przez buffer overflow).
3. W przypadku pojawienia się w sieci zainfekowanego komputera (np. laptopa pracownika mobilnego) wszelkie niedogodności z tym związane dotykają jedynie użytkowników lokalizacji, w której pracuje dany komputer. Ruch przez router (a w przyszłości przez przełącznik sieciowy) jest blokowany do czasu przeprowadzenia procesu sprawdzenia kondycji bezpieczeństwa. W przypadku stosowania przełączników sieciowych jako punktów dopuszczenia/odrzucenia użytkowników oznacza to całkowitą izolację zarażonego hosta od sieci organizacji. Ciekawym efektem jest też oczyszczenie łączy w sieci WAN: jeżeli zainfekowany komputer znajduje się w lokalizacji zdalnej, lokalny router blokuje ruch od zarażonego hosta chroniąc sieci w innych lokalizacjach przed skanowaniem, a tym samym chroni pasmo dostępne dla „zdrowych" hostów.
4. W przypadku krytycznych zagrożeń możliwe jest natychmiastowe wymuszenie ponownego poddania się sprawdzeniu kondycji bezpieczeństwa. Dzieje się tak np. w sytuacji gdy pojawiają się sygnatury z informacjami o wirusach atakujących aplikację krytyczną

w organizacji. Wówczas można wymusić ściągniecie uaktualnienia, jako warunku niezbędnego dla kontynuowania pracy w sieci. Oczywiście, w takich momentach może okazać się konieczne wylogowanie się użytkowników aplikacji na czas uaktualnienia, jednakże jest to jedyny koszt całej operacji.

Najbardziej zaawansowane rozwiązanie

Narzędzia kontroli odporności hosta na atak są jednym z najdynamiczniej rozwijanych kierunków w zakresie bezpieczeństwa sieci i aplikacji. W chwili obecnej ich zastosowanie to już nie kwestia odpowiedzi na pytanie „czy", ale raczej „kiedy". Rozwiązanie Network Admission Control pozwala nie tylko na samą kontrolę odporności, ale także na zintegrowanie rozwiązania z siecią i narzędziami dostępnymi w przełącznikach i routerach dla lepszej kontroli użytkowników. Nawiązanie współpracy pomiędzy Cisco i Microsoft w tym zakresie wskazuje, iż budowanie mechanizmów opartych tylko na infrastrukturze bez zaangażowania aplikacji, jak również tylko i wyłącznie opartych na hostach jest niewystarczające. Należy spodziewać się, iż już w niedługim czasie funkcje podobne do NAC na routerach Cisco pojawią się w innych typach urządzeń, jednakże NAC jest obecnie najbardziej zaawansowanym rozwiązaniem w tym zakresie.

Michał Kraut
pracownik Cisco Systems

Wymagania dla uruchomienia Cisco Network Admission Control:

1. Platforma routerów:
   - ✔ Cisco 83x,
   - ✔ Cisco 1701, 1711, 1712, 1721, 1751, 1760,
   - ✔ Cisco 2600XM,
   - ✔ Cisco 2691,
   - ✔ Cisco 3640A,
   - ✔ Cisco 3660-ENT,
   - ✔ Cisco 3700,
   - ✔ Cisco 7200,
   - ✔ Cisco ISR (seria 1800, 2800, 3800).
2. Oprogramowanie IOS:
   - ✔ IOS 12.3.8T lub nowsze,
   - ✔ IOS Firewall,
   - ✔ IOS Advanced IP Services,
   - ✔ IOS Advanced Security,
   - ✔ IOS Advanced Enterprise.
3. Aplikacje NAC-Enabled:
   - ✔ McAfee VirusScan 7.0; 7.1; 8.0i,
   - ✔ Symantec SAV 9.0,
   - ✔ Symantec SCS 2.0,
   - ✔ Trend Micro OfficeScan CE 6.5 lub nowszy,
   - ✔ IBM Tivoli (w przyszłości).
4. Serwer uwierzytelnienia i autoryzacji:
   - ✔ Cisco Secure Access Control Server 3.3 for Windows,
   - ✔ Cisco Secure Access Control Server 3.3 Solution.

Rozwiązania wspierające korporacyjne sieci

Juniper Networks wprowadziła na rynek nowe rozwiązania wspierające korporacyjne sieci Infranet. Uzupełniają one zarządzanie ruchem sieciowym. Umożliwiając koordynację wymuszania zgodności w sieci z oceną na zakończeniu sieci, uwierzytelnianiem użytkowników oraz bezpiecznym transferem w punkcie końcowym nowe produkty zapewniają organizacjom poziom kontroli wykorzystania i zagrożeń sieci, jaki jest niezbędny dla zapewnienia dobrego funkcjonowania i wysokiej dostępności ich usług.

Wykorzystując najlepszą w swojej klasie technologię obronną w punkcie końcowym oraz funkcjonalność weryfikacji komputera dostępną w Juniper Networks SSL VPN (wirtualna sieć prywatna oparta na protokole SSL) dla rozbudowanych przedsiębiorstw, urządzenie Infranet Controller oraz aplikacja Infranet Agent pozwalają przedsiębiorstwom chronić ich sieci i zakończenia klienckie w odległych i rozproszonych lokalizacjach. Podejście to stanowi odpowiedź na wyzwania związane z sieciami i bezpieczeństwem, jakie stoją obecnie przed przedsiębiorstwami pragnącymi zapewnić powszechny dostęp do sieci, w tym dla ciągle rosnącej liczby użytkowników włączających się do sieci przy pomocy komputerów przenośnych. Tradycyjne podejścia skupiające się na niekompletnych modelach skanowania i blokowania, które powodują powstawanie dziur w bezpieczeństwie i wiążą się z koniecznością ponoszenia wysokich kosztów, nie stanowią odpowiedzi na te wyzwania czy też na problem oprogramowania złośliwego. Podejście Juniper Networks jest zgodne z rozwiązaniami heterogenicznymi i wykorzystuje elementy technologii SSL VPN, firewall oraz IPSec, zapewniając kompleksowe zabezpieczenie sieci.

Bezpieczny dostęp

Nowy Enterprise Infranet Controller umożliwia stosowanie warunkowego dostępu do sieci opartych na uwierzytelnianiu użytkowników oraz weryfikację cech bezpieczeństwa urządzenia w czasie rzeczywistym. Dynamiczny Infranet Agent przyjmuje uwierzytelnienie użytkownika, przeprowadza weryfikację komputera oraz zapewnia opcjonalne uwierzytelniane i szyfrowane przekazanie do bramek wymuszających zgodność sieci. Bramki te zostaną dostarczone w postaci aktualizacji oprogramowania systemów i urządzeń typu firewall NetScreen firmy Juniper Networks. Rozwiązania te są szeroko stosowane w kluczowych miejscach w sieci i podejmują precyzyjne decyzje dotyczące ruchu sieciowego. Odbierając sygnały z urządzenia Infranet Controller i przerywając połączenia od agentów bramki te mogą zapewnić kompleksowe bezpieczeństwo transferu danych, większą kontrolę nad polityką bezpieczeństwa, jak również przejrzystość sieci, bez potrzeby wprowadzania znacznych zmian w infrastrukturze. Zastosowanie nowego urządzenia Juniper Networks Enterprise Infranet Controller przyniesie korzyści podobne jak SSL VPN, lecz na znacznie większą skalę, nie pozwalając niezgodnym komputerom włączać się do sieci korporacyjnej i zapewniając kontrolę ruchu sieciowego w przedsiębiorstwie.

– *Specjaliści od bezpieczeństwa sieci doskonale zdają sobie sprawę, iż obecnie oferowane rozwiązania nie rozwiązują problemu wciąż rosnącej liczby ataków ani nie odpowiadają na rosnące wymagania ewoluujących sieci* – zauważa **Andrew Harding**, dyrektor w dziale Zarządzania Produktami Juniper Networks. – *Juniper uporał się już z tym problemem opracowując rozwiązanie SSL VPN dla rozbudowanych przedsiębiorstw, które zapewnia bezpieczny dostęp różnorodnym użytkownikom, łączącym się z różnych miejsc przy pomocy zabezpieczonych lub niezabezpieczonych urządzeń. Dzięki połączeniu funkcji obronnych w odniesieniu do zakończenia sieci naszej platformy SSL VPN ze skalowalnością wydajnościową naszych platform Firewall/VPN możemy rozszerzyć model wykorzystania i bezpieczeństwo SSL VPN dla dostępu zdalnego oraz ekstranetów na rozległe sieci korporacyjne.*

Kompatybilność z innymi rozwiązaniami

Enterprise Infranet Framework uzupełnia współpracę Juniper Networks z firmą Microsoft nad Network Access Protection (zabezpieczenie dostępu do sieci) oraz działania standaryzacyjne, takie jak Trusted Network Connect Subgroup (podgrupa ds. łączenia zaufanych sieci) organizacji Trusting Computing Group. Starania te stanowią następny etap na drodze do integracji polityk i wymuszania zgodności użytkownika, aplikacji i sieci w sposób bezproblemowy za pomocą otwartych, heterogenicznych rozwiązań ułatwiających zapewnienie bezpieczeństwa sieci.

Opracowano na podstawie materiałów firmy Juniper Networks

Budowa i bezpieczeństwo sieci Wi-Fi

Budowa bezpiecznej sieci bezprzewodowej w firmie, która zapewni poufną transmisję danych oraz możliwość kontroli dostępu, nie kończy się na zakupie kart bezprzewodowych oraz punktów dostępowych. Wprowadzenie mechanizmów bezpieczeństwa sieci bezprzewodowej w dużej firmie wiąże się z koniecznością zakupu serwera centralnej autoryzacji użytkowników RADIUS oraz, w zależności od decyzji o zastosowaniu konkretnych mechanizmów bezpieczeństwa, dodatkowych systemów, takich jak infrastruktura klucza publicznego. Może się zdarzyć, iż powyższe systemy są już zainstalowane i wykorzystywane w firmie do innych celów, jak np. zdalny dostęp poprzez system Remote Access Server lub poprzez tunele VPN. W takim przypadku wdrożenie sieci bezprzewodowej jest znacznie prostsze.

Jakie mechanizmy bezpieczeństwa dla sieci bezprzewodowych powinno się zatem stosować w sieciach korporacyjnych? Po pierwsze, muszą być to mechanizmy standardowe, które wspierane są przez wielu producentów, tak aby była możliwość wyboru dostawcy urządzeń. Jednym ze standardów kontroli dostępu do sieci jest standard IEEE 802.1x, czyli tzw. Network Login. Zaletą tego standardu jest możliwość wykorzystania go do kontroli dostępu do sieci bezprzewodowej, jak również sieci przewodowej, co pozwala na stosowanie jednakowych mechanizmów i systemów do kontroli dostępu do sieci. W ramach standardu IEEE 802.1x zdefiniowano możliwość korzystania z rozszerzonych protokołów autoryzacji użytkowników. Najczęściej spotykane mechanizmy autoryzacji w ramach IEEE 802.1x to: EAP-MD5, EAP-TLS, EAP-TTLS oraz PEAP. Wybierając jeden z powyższych standardów do autoryzacji dostępu użytkowników do sieci musimy zapewnić obsługę tego protokołu przez kartę sieciową lub system operacyjny po stronie klienta oraz przez serwer RADIUS, który jest wymagany przez standard IEEE 802.1x. Punkt dostępowy musi obsługiwać tylko protokół IEEE 802.1x, gdyż protokoły rozszerzonej autoryzacji użytkowników są transportowane w ramach IEEE 802.1x.

Protokół EAP-MD5 jest najprostszym rozszerzonym protokołem autoryzacji użytkownika. Wymaga on po stronie klienckiej podania nazwy użytkownika i hasła. Nazwa użytkownika i hasło sprawdzane są w centralnym systemie autoryzacji RADIUS, gdzie podejmowana jest decyzja, czy wpuścić użytkownika do sieci, czy nie. EAP-MD5 zapewnia jedynie autoryzację użytkownika i tutaj rola tego protokołu się kończy. EAP-MD5 nie zapewnia negocjacji kluczy oraz algorytmu szyfracji, tak więc po procesie autoryzacji transmisja danych nie jest szyfrowana lub może być szyfrowana, ale jedynie przez np. protokół szyfrację WEP ze statycznym, współdzielonym kluczem szyfracji.

Protokół EAP-TLS jest na dzień dzisiejszy najlepszym mechanizmem autoryzacji w sieci bezprzewodowej. Do procesu autoryzacji oraz wymiany kluczy szyfracji wykorzystuje on cyfrowe certyfikaty, które muszą być wygenerowane dla każdej stacji końcowej oraz dla serwera RADIUS. Rozwiązanie takie pozwala na wzajemne uwierzytelnienie klienta oraz punktu dostępowego i negocjację kluczy szyfracji. Niestety, zastosowanie tego protokołu wymaga generacji cyfrowych certyfikatów i zarządzania nimi, co wiąże się z koniecznością uruchomienia systemu klucza publicznego w ramach firmy i, niestety, jest związane z dodatkowymi kosztami.

Kolejne dwa protokoły rozszerzonej autoryzacji EAP-TTLS i PEAP są pewnym rozwiązaniem dla zmniejszenia kosztów związanych z koniecznością ge-

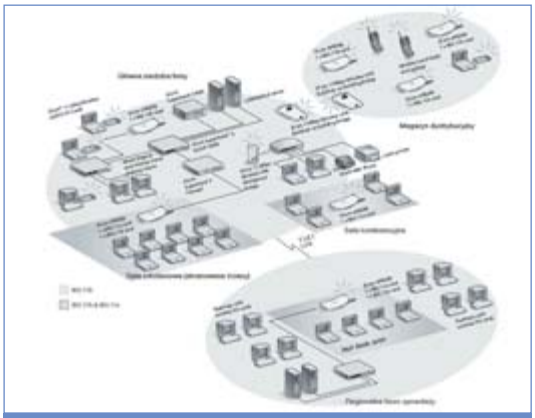
Artur Borowski – dyrektor generalny 3Com w Polsce:

– Rynek rozwiązań bezprzewodowych sukcesywnie rośnie, głównie w obszarze rozwiązań dla klientów indywidualnych – SOHO. W tym segmencie największym powodzeniem cieszą się najprostsze rozwiązania. Tę swoistą niszę wykorzystują operatorzy telekomunikacyjni oferując np. zestawy łączy ADSL z koncentratorem bezprzewodowym. Dla operatorów promowanie takiego rozwiązania to świetna metoda na utrzymanie istniejących i pozyskiwanie nowych klientów. Dla użytkowników, w dobie powszechności komputerów przenośnych, wyjątkowo przyjazna metoda dostępu do Internetu. Wkrótce rozwiązania Wi-Fi będą standardem w większości domów i mieszkań. Za sprawą operatorów GSM obserwujemy również wzrost liczby hot-spotów. W wielu miejscach publicznych można już dziś korzystać z Internetu przez Wi-Fi. Każdy z operatorów ma w tym obszarze swoje pomysły i rozwiązania. Upowszechnienie bezprzewodowego dostępu do Internetu stwarza też szansę na nowe kontrakty dla producentów rozwiązań bezprzewodowych. Należy się zatem spodziewać dalszego wzrostu sprzedaży urządzeń Wi-Fi. Wraz z umacnianiem się wersji 11g, Wi-Fi winno znaleźć się również w rozwiązaniach dla instytucji – wymagających wyższych przepustowości i bezpieczeństwa transmisji. Na ten sektor liczy 3Com.

neracji cyfrowych certyfikatów dla każdej stacji końcowej. Powyższe standardy wymagają cyfrowego certyfikatu tylko dla serwera RADIUS. Cyfrowy certyfikat na serwerze RADIUS pozwala na otworzenie bezpiecznego tunelu, wewnątrz którego przeprowadzana jest autoryzacja z wykorzystaniem innych protokołów autoryzacyjnych. Może to być jeden z protokołów EAP lub protokoły nieco starsze typu PAP, CHAP, MS-CHAP, MS-CHAP v.2. Podobnie jak w przypadku protokołu EAP-TLS, oprócz autoryzacji użytkownika do sieci zapewniana jest również negocjacja kluczy szyfracji do zapewnienia bezpiecznej transmisji bezprzewodowej.

Oprócz autoryzacji użytkownika w sieci bezprzewodowej z wykorzystaniem protokołu IEEE 802.1x oraz jednego ze wspomnianych protokołów rozszerzonej autoryzacji EAP-MD5, EAP-TLS, EAP-TTL lub PEAP konieczne jest wybranie algorytmu szyfracji danych w sieci bezprzewodowej. Mamy do wyboru w zasadzie trzy możliwości: szyfrację WEP, szyfrację WPA (TKIP) oraz szyfrację AES. Oczywiście, najlepszym wyborem będzie zastosowanie szyfracji AES (*Advanced Encryption Standard*), która jako następca szyfracji 3DES oferuje największy poziom bezpieczeństwa. Trzeba jednak zwrócić uwagę, że nie wszystkie urządzenia dostępne na rynku oferują szyfrację AES. W tym przypadku konieczne będzie zastosowanie szyfracji WPA lub ostatecznie szyfracji WEP. Szyfracja WPA oraz szyfracja WEP mogą być używane bez konieczności stosowania kontroli dostępu IEEE 802.1x i algorytmów rozszerzonej autoryzacji. Tego typu rozwiązania nie powinny być jednak stosowane do zabezpieczania transmisji danych w sieciach korporacyjnych.

Bardzo istotnym mechanizmem w korporacyjnych punktach dostępowych jest protokół IAPP (*Inter Access Point Protocol*), nad którym pracę prowadzi grupa standaryzacyjna 802.11f. Proszę zwrócić uwagę, że w przypadku wykorzystania mechanizmu network login IEEE 802.1x oraz protokołów rozszerzonej autoryzacji typu EAP-TLS, EAP-TTLS i PEAP generowane są klucze szyfracji do zapewnienia bezpiecznej transmisji danych między punktem dostępowym a kartą kliencką. Po autoryzacji klucz szyfracji jest znany karcie bezprzewodowej oraz konkretnemu punktowi bezprzewodowemu, do którego był dołączony klient. Przejście klienta bezprzewodowego z jednego punktu dostępowego do drugiego wiąże się z koniecznością ponownej autoryzacji użytkownika, gdyż drugi punkt dostępowy nie ma żadnych informacji o danym kliencie. Standard IEEE 802.11f definiuje sposób wymiany informacji pomiędzy



Przykładowe rozwiązanie infrastruktury bezprzewodowej z wykorzystaniem urządzeń firmy 3Com

punktami dostępowymi o autoryzacji klienta bezprzewodowego eliminując konieczność ponownej autoryzacji.

Innym mechanizmem przydatnym w korporacji może być automatyczny przydział klienta bezprzewodowego do konkretnej sieci wirtualnej w zależności od podanej nazwy użytkownika.

Podsumowując: dla zastosowań korporacyjnych sieci bezprzewodowych powinniśmy stosować protokół IEEE 802.1x z jednym z bezpiecznych mechanizmów autoryzacji EAP-TLS, EAP-TTLS lub PEAP oraz szyfracją AES lub WPA.

Firma 3Com produkuje aktualnie następujące punkty dostępowe dla zastosowań korporacyjnych: AccessPoint 8250, AccessPoint 8500, AccessPoint 8750 oraz AccessPoint 7250. Trzy pierwsze punkty dostępowe to tak faktycznie jeden dwuradiowy punkt dostępowy z różnym wyposażeniem. AccessPoint 8250 ma zainstalowany jeden moduł radiowy IEEE 802.11g, który jest wstecznie zgodny ze standardem IEEE 802.11b oraz ma jeden slot wolny na instalację dodatkowego modułu. AccessPoint 8500 jest wyposażony w jeden moduł radiowy IEEE 802.11a oraz jeden slot wolny. W Access-Point 8750 zainstalowano dwa moduły: IEEE 802.11g oraz IEEE 802.11a. AccessPoint 7250 jest jednoradiowym punktem dostępowym wyposażonym w interfejs radiowy IEEE 802.11g. Wszystkie cztery wymienione punkty dostępowe obsługują wymienione w artykule mechanizmy autoryzacji użytkowników, szyfracji danych (wraz z AES – *Advanced Encryption Standard*) i mechanizmy dodatkowe, takie jak obsługa sieci wirtualnych w sieci bezprzewodowej oraz protokół komunikacji między punktami dostępowymi IAPP.

Jako urządzenia dla klientów bezprzewodowych 3Com proponuje karty 3Com Wireless 11a/b/g PC Card with XJACK Antenna (3CRPAG175) do komputerów przenośnych wyposażonych w gniazda PC Card oraz 3Com Wireless 11a/b/g PCI Card (3CRDAG675) do komputerów stacjonarnych wyposażonych w złącza PCI.

Opracowano na podstawie materiałów firmy 3com

Niniejszy artykuł ukazał się w INFOTELU NR 6/2004

Ochrona danych w internecie

Internet otwiera przed nami wielkie możliwości, ale korzystanie z niego nie jest pozbawione pewnego ryzyka. W drodze do pełnego wykorzystania internetu wielką rolę do odegrania mają technologie ochrony danych. Każdy użytkownik Internetu musi chronić własne zasoby przed niepowołanym dostępem z zewnątrz.

Zagadnienia bezpieczeństwa na styku z internetem nabierają innego wymiaru, jeśli nasza firma decyduje się prowadzić przez sieć swoje interesy. Internet daje tu szczególnie atrakcyjne możliwości. Od kilku lat na naszych oczach dokonuje się ewolucja stron internetowych, które przestają pełnić funkcje tylko reklamowe, a stają się miejscem przeprowadzania transakcji e-commerce, wartych już dziś setki miliardów dolarów. Internet jest nowym teatrem dla prowadzenia interesów, a wiążąca się z tym redukcja kosztów firm powoduje, że uczestnictwo w gospodarce internetowej przestaje być opcją, a staje się koniecznością. To, co jeszcze dziś jest źródłem przewagi konkurencyjnej, jutro będzie obowiązującym standardem. Niestety, powszechnej adaptacji rozwiązań internetowych często towarzyszy ignorowanie problemów związanych z zapewnieniem bezpieczeństwa. Nagłaśniane ostatnio przez media ataki hackerów na popularne sklepy internetowe unaoczniły fakt, że nawet najwięksi reprezentanci nowej gospodarki nie ustrzegli się rażących zaniedbań w tej dziedzinie. Tymczasem długofalowe powodzenie przedsięwzięcia wymaga zdobycia zaufania klientów i partnerów przez zapewnienie ich transakcjom maksymalnego bezpieczeństwa. Problemem, przed jakim stoją firmy chcące budować bezpieczne rozwiązania internetowe, nie jest brak dostępnych rozwiązań, lecz integracja dostępnych środków technicznych w spójny system, gdyż żadne pojedyncze urządzenie nie zapewni pożądanego bezpieczeństwa. Firma Cisco zaprojektowała całościowe rozwiązanie bezpieczeństwa dla firm korzystających z internetu i wykorzystujących sieć dla prowadzenia działalności gospodarczej.

Wymagania stawiane przed bezpiecznym stykiem z Internetem

Infrastruktura sieciowa na styku firmy z internetem powinna zapewniać użytkownikom:

- ✔ bezpieczeństwo,
- ✔ wydajność,
- ✔ skalowalność,
- ✔ niezawodność i wysoką dostępność.

Bezpieczeństwo

Internet przynosi nam oprócz nowych możliwości również nowe zagrożenia. Najpowszechniejsze problemy bezpieczeństwa to świadome lub przypadkowe niszczenie albo modyfikacja danych (bądź podczas transmisji, bądź rezydujących na serwerach), zablokowanie usług (znane jako atak typu *Denial of Service*) przez zalew fikcyjną informacją zużywającą zasoby sieci i komputerów, podszywanie się pod użytkowników bądź pod serwer, wykonywanie nieautoryzowanych transakcji bez odpowiednich uprawnień.

Mając świadomość faktu, że nie istnieje żadne pojedyncze rozwiązanie gwarantujące bezpieczeństwo, styk z internetem należy zaprojektować maksymalnie, wykorzystując dostępne technologie ochrony danych, takie jak:

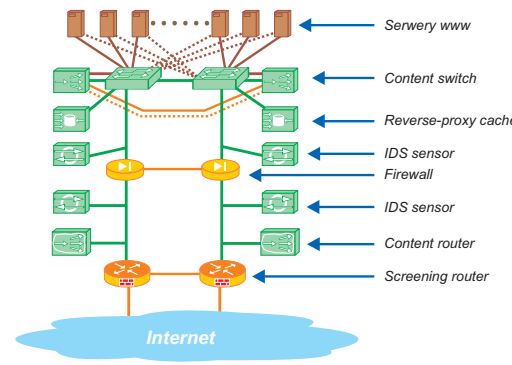
- ✔ kontrola dostępu – np. firewall Cisco PIX, router z oprogramowaniem IOS Firewall Feature Set,
- ✔ detekcja ataków – np. Cisco Secure IDS,
- ✔ kontrola tożsamości – np. Cisco Secure ACS, SSL,
- ✔ poufność i integralność – np. IPsec, SSL,
- ✔ autentyczność – podpisy cyfrowe, certyfikaty cyfrowe.

Wydajność

Maksymalizacja wydajności zwykle stoi w sprzeczności z chęcią zapewnienia maksymalnego bezpieczeństwa. Odpowiedni dobór urządzeń, takich jak router brzegowy, firewall, sonda IDS pozwala na częściowe rozwiązanie tego dylematu. Wydajność całego rozwiązania styku z Internetem jest taka, jaka jest wydajność jego najsłabszego ogniwa, tak więc szczególne znaczenie ma poprawne zaprojektowanie całego rozwiązania, tak aby zidentyfikować wszelkie potencjalne wąskie gardła, a następnie je usunąć.

Skalowalność

Skalowalność styku z Internetem to skalowalność urządzeń sieciowych, a w przypadku rozwiązań e-commerce również skalowalność serwerów WWW. W obu przy-



Bezpieczny styk z internetem

padkach pełną, liniową skalowalność można uzyskać tylko poprzez dodawanie urządzeń sieciowych (np. firewalli) i serwerów WWW oraz rozkład obciążenia pomiędzy nimi. Algorytm rozkładu obciążenia powinien reagować na rzeczywiste obciążenie urządzeń. W przypadku rozwiązań typu e-commerce dodatkową trudność sprawia konieczność utrzymywania integralności transakcji poprzez zapewnienie, że wszystkie sesje w ramach jednej transakcji będą obsługiwane przez ten sam serwer. Wszystkie te wymagania realizuje technologia nazywana *content switching*, obecna na takich urządzeniach, jak Cisco Local Director i Cisco Content Smart Switch.

Niezawodność i wysoka dostępność

Niezawodność styku z internetem jest zawsze bardzo istotna,. Dla zastosowań typu e-commerce każda minuta przestoju oznacza wymierne straty. Wysoka dostępność, czyli zdolność sieci do samonaprawy wymaga pełnej redundancji wszystkich elementów sieciowych, łącznie z serwerami. Dodatkowo dostępne muszą być technologie pozwalające na szybką identyfikację awarii i natychmiastowe, najlepiej niezauważalne dla użytkownika, przełączenie na urządzenie zapasowe. Dobrze też, jeśli w czasie normalnej pracy element zapasowy jest wykorzystywany odciążając urządzenie podstawowe. W przypadku serwerów detekcja awarii powinna polegać nie tyle na weryfikacji czy dany serwer pracuje, ale na weryfikacji czy dany serwer aktualnie posiada plik żądany przez użytkownika (tę funkcję realizuje technologia *content switching*). Poniżej wymienione są technologie spełniające większość przedstawionych wymagań:

- ✔ redundancja operatorów internetowych (ISP) – technika *multihoming* i protokół BGP4,
- ✔ redundancja przyłącza do operatora internetowego – technika *multihoming* i protokół BGP4,
- ✔ redundancja routerów brzegowych – technika Cisco HSRP oraz technika *multihoming* i protokół BGP4,
- ✔ redundancja firewalli – funkcja *statefull failover* firewalla Cisco PIX lub w przypadku farmy firewalli technologia *content switching*,
- ✔ redundancja serwerów WWW – technologia *content switching*.

W przypadku rozwiązań e-commerce dodatkowym zabezpieczeniem może być stworzenie dwóch, geograficznie oddalonych centrów komputerowych, każdego z własnym stykiem z internetem. Dla użytkownika oba centra powinny być reprezentowane przez jeden adres URL. Jest to możliwe dzięki technologii *content routing*, wykorzystującej cechy protokołu DNS i podejmującej optymalne decyzje, do którego centrum skierować użytkownika na podstawie takich parametrów, jak obciążenie komputerów w centrach czy ich odległość od użytkownika. Technologia *content routing* jest dostępna na urządzeniach Cisco Distributed Director i Cisco Content Smart Switch.

Elementy składowe bezpiecznego styku z Internetem

Screening router

Screening router jest to nazwa nadawana routerowi łączącemu firmę z Internetem, stanowiącemu jednocześnie pierwszą linię obrony. Router ten powinien odfiltrowywać niepożądany ruch przed dostaniem się do sieci firmy. Dzięki oprogramowaniu IOSTM Firewall Feature Set dla routerów Cisco, filtracja dokonywana przez router nie musi ograniczać się do prostego sprawdzania zawartości nagłówka każdego pakietu, ale może mieć charakter kontekstowy. Router identyfikuje wtedy konwersacje nawiązywane w sieci i interpretuje znaczenie każdego pakietu w kontekście nawiązanych konwersacji (technika ta nosi nazwę *Context Based Access Lists* – CBAC). Podnosi to znacznie pewność działania filtracji i zmniejsza ryzyko jej przełamania, a sam router nabiera charakteru prostego firewalla. *Screening router* będzie dobrze pełnił swoją funkcję, jeśli sam będzie dobrze zabezpieczony przed dostępem ze strony osób niepożądanych.

Firewall

Firewall stanowi kluczowy element zabezpieczający firmę przed zewnętrznym światem Internetu. Ponosi on główną odpowiedzialność za bezpieczeństwo sieci wewnętrznej firmy i to on realizuje właściwe mechanizmy ochrony danych. Firewall Cisco PIX, typowo skonfigurowany, wykorzystuje do zabezpieczenia sieci wewnętrznej firmy następujące technologie:

- ✔ Adaptive Security Algorithm monitorujący konwersacje w sieci i powodujący, że firewall działa w trybie tzw. *stateful security*,
- ✔ translacja adresów sieciowych (NAT) dla ruchu wchodzącego i wychodzącego,
- ✔ obrona przed atakami typu *Denial of Service* (funkcja nazywana również *Sunc Flood Defend*),
- ✔ technika *cut-through proxy* umożliwiająca weryfikację tożsamości użytkownika przy jednoczesnym zachowaniu wydajności sieci,
- ✔ filtracja ruchu w oparciu o adres URL,
- ✔ filtracja apletów Javy i elementów ActiveX.

Intrusion Detection System

Intrusion Detection System to rozwiązanie pozwalające na monitoring w czasie rzeczywistym zdarzeń zachodzących w sieci oraz, w razie potrzeby, reagujące na niepożądane zjawiska. Generalnie umożliwia on wykluczenie z monitorowanego segmentu sieci intruza próbującego jakiejkolwiek aktywności. W skład rozwiązania wchodzi sonda (Cisco Secure IDS Sensor), będąca urządzeniem monitorującym konkretny segment sieci lokalnej, oraz konsola operatorska (Cisco Secure IDS Director), stanowiąca aplikację wizualizującą w czasie rzeczywistym informacje o atakach w sieci. Kluczowym

elementem rozwiązania jest baza danych z wzorcami znanych ataków (tzw. sygnaturami) pozwalająca na ich identyfikację.

W typowej implementacji systemu IDS sondy rozmieszcza się przed i za każdym firewallem. Dzięki temu otrzymujemy pełny obraz jego skuteczności, gdyż dostajemy informacje o wszystkich atakach na naszą sieć oraz o tych z nich, które zdołały przeniknąć przez firewall. Aplikację Cisco Secure IDS Director umieszcza się w sieci wewnętrznej (za firewallem), a sondy komunikują się z nią wydzielonymi łączami. Sama sonda nie stanowi osłabienia systemu bezpieczeństwa, gdyż jest zupełnie niewidoczna w sieci, nie jest też wąskim gardłem, gdyż jedynie podsłuchuje ruch w segmencie Ethernet, nie uczestnicząc w transmisji.

Content Switch

Content Switch to specjalizowane urządzenie dla środowisk e-commerce i portali internetowych. Jego zadaniem jest skierowanie żądania klienta do właściwego serwera WWW lub urządzenia typu *cache*. Decyzja o tym, do którego serwera skierować żądanie, podejmowana jest w oparciu o szereg konfigurowalnych parametrów:

- ✔ dostępność serwera,
- ✔ obciążenie serwera,
- ✔ czas odpowiedzi z serwera,
- ✔ dostępność żądanego pliku na serwerze,
- ✔ parametry sieciowe warstwy 3 i 4 żądania (adres IP, port TCP, itp.),
- ✔ parametry sieciowe warstwy 5, 6 i 7 żądania, takie jak: adres URL, identyfikator sesji SSL czy obecne w żądaniu Cookie.

W sytuacji, gdy wszystkie dostępne serwery są przeciążone, przełącznik może uruchomić dodatkowe serwery lub urządzenia typu *cache*, będące w rezerwie, kopiując na nie szczególnie często żądane pliki i dodając je do farmy serwerów do czasu zmniejszenia „popytu".

Rezultatem działania *content switcha* jest minimalizacja czasu odpowiedzi z serwera obserwowana przez klienta i eliminacja okresów niedostępności usług. Ubocznym efektem jego pracy jest dodatkowa ochrona serwerów WWW, gdyż *content switch*, podobnie jak firewall, działa w trybie *stateful security*. Przełączniki te, np. Cisco Content Smart Switch 11000 lub Cisco Local Director umieszczane są bezpośrednio przed serwerami WWW. W przypadku rozbudowanych *data center* możliwe jest stworzenie wielopoziomowej hierarchii przełączników typu *content switch*.

Content Routing

Content Router znajduje swoje zastosowanie w sytuacji budowy wielu, geograficznie oddalonych, centrów danych. Jego zadaniem jest skierowanie żądania klienta do właściwego centrum. Router może skorzystać tu z kombinacji następujących kryteriów:

- ✔ dostępność żądanego pliku w danym *data center*,
- ✔ obciążenie danego *data center*,
- ✔ odległość *data center* od użytkownika, który wygenerował żądanie,
- ✔ aktualny stan sieci.

Najczęściej stosowaną przez *content router* techniką skierowania klienta do wybranego *data center* jest współpraca z systemem DNS i zwrócenie powiązania stosowanego przez użytkownika adresu URL z wybranym adresem IP właściwego *data center*. Proces ten jest zupełnie niezauważalny z punktu widzenia klienta. Efektem działania *content routera* jest minimalizacja czasu odpowiedzi obserwowana przez klienta i eliminacja okresów niedostępności usług.

Cache

Integralnym elementem łącza internetowego każdej firmy powinien być *cache* internetowy. Urządzenie to znajduje zastosowanie zarówno w przypadku korzystania z internetu przez pracowników naszej firmy, jak i w przypadku udostępniania naszych serwerów WWW użytkownikom Internetu, jednak jego rola jest w każdej z tych sytuacji różna.

W pierwszym przypadku urządzenie *cache* działa w trybie *transparent caching*. Polega on na niewidocznym dla użytkowników przekierowywaniu odwołań do serwisów internetowych i skierowywaniu ich do urządzania *cache*. Urządzeniem przekierowującym odwołania jest najczęściej router znajdujący się na styku z internetem (*screening router*). *Cache* w imieniu użytkownika znajduje informację na Internecie i odpowiada na żądanie.

Celem działania *transparent cache* jest skrócenie czasu odpowiedzi dla użytkowników i zmniejszenie obciążenia łączy transmisją powtarzających się informacji.

W przypadku drugim urządzenie *cache* działa w trybie *reverse-proxy caching*. W tym trybie *cache* obsługuje żądania klientów w imieniu danej grupy serwerów WWW. Celem działania *reverse cache* jest odciążenie serwerów WWW z transmisji pewnych, najczęściej statycznych, informacji. Użytkownicy są w sposób przezroczysty, ale wybiórczy przekierowywani do urządzenia *cache*, a urządzeniem przekierowującym jest najczęściej *content switch*.

Opracowano na podstawie materiałów firmy Cisco Systems

Niniejszy artykuł ukazał się w INFOTELU NR 1/2004

Nortel WLAN 2300

Nortel Networks zaprezentował nowe portfolio produktów do zastosowań w budowie sieci WLAN – serię 2300, która do atutów swojej poprzedniczki – serii 2200 dodała elementy jakże istotne dla użytkowników korporacyjnych: mniejsze koszty eksploatacji i większą skalowalność.

Oferowana przez Nortel nowa seria WLAN 2300 ma zapewnić realizację wysokiej jakości aplikacji w zakresie transmisji głosu, danych i multimediów – dzięki czemu bezprzewodowa sieć LAN staje się podstawową formą komunikacji dla przedsiębiorstw. Zapewniające uzyskanie najlepszego na rynku modelu w zakresie całkowitego kosztu posiadania oraz niespotykaną wcześniej łatwość instalacji i zarządzania oferowane przez Nortel rozwiązanie składa się z następujących elementów:

- ✔ WLAN 2330 – Access Point;
- ✔ WLAN 2300 – System Zarządzania;
- ✔ WLAN 2350 – Security Switch;
- ✔ WLAN 2360 – Security Switch;
- ✔ WLAN 2370 – Security Switch;
- ✔ WLAN 2380 – Security Switch.

– Specjaliści oczekują zapewnienia im możliwości połączenia się z siecią w sposób niezawodny i bezpieczny, niezależnie od tego, czy używają telefonu komórkowego, notatnika elektronicznego (PDA), WLAN, czy aparatu telefonicznego IP – powiedział ***Aaron Vance****, starszy analityk Synergy Research Group. – Nortel ma w swojej ofercie rozwiązania w zakresie systemów łączności bezprzewodowej, a nowa oferta pomoże klientom uprościć zarządzanie i obniżyć ogólny poziom kosztów. Dodatkowo strategia firmy Nortel w zakresie wprowadzania funkcji łączności bezprzewodowej do produktów pracujących w sieci przewodowej jest zgodna z kierunkiem, w którym zmierza rynek.*

Celem naszej wizji rozwoju łączności mobilnej jest podniesienie poziomu jakości obsługi użytkowników oraz przyczynienie się do wzrostu poziomu wydajności pracy i sprawności działania naszych klientów – **powiedział Malcolm Collins**, prezes Enterprise Networks Nortel. *– Przy pomocy oferowanych przez Nortel rozwiązań w zakresie łączności mobilnej klienci mogą realizować bezpieczne, konwergentne usługi sieciowe w sposób identyczny z dostępnymi za pośrednictwem infrastruktury przewodowej. Wprowadzenie tej nowej oferty produktów pozwala nam na zaoferowanie naszych rozwiązań w zakresie łączności bezprzewodowej dla pełnej gamy klientów, poczynając od dostawców usług, dużych korporacji, aż po małe przedsiębiorstwa.*

– Nortel chce uzyskać pozycję lidera na szybko zmieniającym się rynku między innymi dzięki wprowadzaniu funkcji w zakresie łączności bezprzewodowej do produktów pracujących w sieci przewodowej – dodał Collins. *– Będziemy realizować aplikacje i usługi w sposób najbardziej wygodny i wydajny, aby pomóc wszystkim klientom podnieść poziom wydajności pracy oraz obniżyć koszty.*

Malcolm Collins, prezes Enterprise Networks Nortel

Elementem kluczowym dla realizacji tej wizji jest nowa oferta produktów przeznaczonych do pracy w sieci WLAN, składająca się z serii WLAN 2300. Pozwala ona spełnić potrzeby w zakresie łączności mobilnej klientów zaliczanych do wszystkich segmentów rynku, poczynając od małych i średnich firm, aż po duże przedsiębiorstwa i dostawców usług. Zakres skalowalności tych urządzeń zapewnia możliwość rozbudowy systemów w zakresie łączności mobilnej wraz z rozwojem klientów, rozszerzających swoje systemy w celu zapewnienia obsługi nowych użytkowników i aplikacji, przy jednoczesnym zapewnieniu ochrony początkowych inwestycji.

Nowa seria WLAN 2300 to rozwiązanie w zakresie WLAN zapewniające:

- ✔ wyższy poziom wydajności pracy uzyskiwany dzięki posiadanym funkcjom oraz poziomowi odporności na uszkodzenia pozwalającemu na realizację wysokiej jakości aplikacji głosowych i multimedialnych za pośrednictwem sieci WLAN;
- ✔ niższy całkowity koszt, uzyskany dzięki zredukowaniu liczby elementów sieciowych wymagających zainstalowania i zarządzania;
- ✔ większy zakres elastyczności – seria WLAN 2300 jest zoptymalizowana pod kątem zastosowania w sieci łączności mobilnej we współpracy z dowolnym urządzeniem – WLAN Handset, Mobile Voice Client, przenośne urządzenie Blackberry, przenośny komputer. Ponadto szeroki zakres skalowalności, pozwalający na obsługę zarówno tylko kilku, jak również tysięcy punktów dostępowych za pośrednictwem szeregu sieci;
- ✔ większe możliwości w zakresie zarządzania dzięki zaawansowanym funkcjom służącym do wspomagania procesu eksploatacji oraz narzędziom pozwalającym na monitorowanie i tworzenie raportów;
- ✔ wysoki poziom bezpieczeństwa dzięki zastosowaniu architektury WLAN oraz najlepszych na rynku rozwiązań w zakresie bezpieczeństwa.

Opracowano na podstawie materiałów firmy Nortel Networks

Odporna sieć

Sieci zabezpieczone w 100 procentach nie istnieją. Zawsze jest jakieś ryzyko włamania i wycieku ważnych danych. Można je jednak minimalizować poprzez właściwą budowę i odpowiednią konfigurację zabezpieczeń danej sieci.

Podstawową zasadą bezpieczeństwa jest tworzenie wielu niezależnych, lecz współpracujących ze sobą warstw. Czasy, gdy do zapewnienia spokoju użytkownikom (i administratorowi) wystarczał zwykły firewall, są już zamierzchłą przeszłością. Wraz ze wzrostem stopnia złożoności ataków nieuchronny był wzrost złożoności zabezpieczeń.

Jeżeli ktoś uważa, że zapewnienie bezpieczeństwa jest bardzo łatwe, to błądzi. Praktycznie każdy element sieci może być celem ataku i dlatego trzeba go odpowiednio zabezpieczyć. Przyglądając się naszym sieciom, a także czytając zalecenia pisane przez ekspertów (np. cykl dokumentów opisujących architekturę bezpieczeństwa SAFE autorstwa Cisco) możemy wyróżnić kilka głównych grup urządzeń i mechanizmów zabezpieczeń:

- ✔ **urządzenia końcowe** – czyli stacje robocze, serwery, laptopy, ale także PDA. To one są źródłami i celami transmisji danych i to one padają ofiarą wirusów, robaków, włamań, kradzieży danych. Systemy zabezpieczeń urządzeń końcowych muszą dzisiaj wyprzedzać o krok wirusy i zamiast polegać na sygnaturach powinny rozpoznawać charakterystyczne objawy problemów i zapobiegać im jeszcze zanim problemy zostaną w pełni zdiagnozowane przez ludzi. Przykładem takiego nowoczesnego zabezpieczenia dla systemów operacyjnych Microsoft Windows, Linux i Solaris jest Cisco Security Agent;
- ✔ **firewalle** – wciąż niezbędny składnik systemu zabezpieczeń, pozwalający kontrolować przepływ danych pomiędzy zdefiniowanymi segmentami sieci, działający jak grodzie wodoszczelne. Firewalle wymuszają część polityki bezpieczeństwa dotyczącą komunikacji i dostępu, a także weryfikację poprawności transmisji dla podstawowych protokołów sieciowych. W ofercie Cisco znajdują się zarówno firewalle dedykowane (seria Cisco Secure PIX), moduły do przełączników LAN (Cisco Firewall Service Module), jak i zintegrowane firewalle w routerach (Cisco Secure IOS Firewall);
- ✔ **sieci lokalne** – oprócz zagrożeń z zewnątrz sieci firmowe narażone są na ataki pochodzące z wewnątrz sieci. Ataki takie mogą być wymierzone przeciwko urządzeniom końcowym bądź samej infrastrukturze sieciowej. Udany atak może oznaczać utratę danych bądź też brak możliwości korzystania z sieci, co często bywa równie dokuczliwe. Aby zmniejszać ryzyko takich ataków, wskazane jest zastosowanie wyrafinowanych mechanizmów zabezpieczających np. przed atakami na serwery DHCP, przed podszywaniem się pod inne komputery czy też przed podsłuchiwaniem ruchu (wbrew popularnemu mniemaniu stosowanie przełącznika samo w sobie nie jest zabezpieczeniem). Funkcje takie są zaimplementowane na przełącznikach Catalyst firmy Cisco;
- ✔ **sieci bezprzewodowe** – radiowa transmisja danych to kolejna bolączka administratorów. Niesłychanie łatwe do podsłuchania, co w przypadku większości popularnych zabezpieczeń prowadzi jednak do przełamania kluczy szyfrujących czy dostępu do sieci przez nieupoważnione osoby. Dopiero połączenie zaawansowanych systemów kluczy dynamicznych (np. EAP-FAST, TKIP) i innych mechanizmów dostępnych w ramach programu Cisco Certified Wireless Extensions (CCX) pozwala na podniesienie poprzeczki powyżej poziomu osiąganego przez dzisiejszych włamywaczy;
- ✔ **zapobieganie atakom sieciowym** – czyli wykrywanie w ruchu sieciowym pewnych charakterystycznych sygnatur to domena sond wykrywających ataki (IDS – *Intrusion Detection System*), a raczej ich najnowszej generacji (IPS – *Intrusion Protection System*), która oprócz wykrywania ataków potrafi także podjąć działania zapobiegawcze, na przykład przerwać transmisję sieciową lub nawet przekonfigurować inne urządzenia sieciowe (routery, firewalle), aby zabronić atakującemu dostępu do sieci. Zapobiec takim atakom można dzięki dedykowanym sondom Cisco IDS, modułom do przełączników LAN (IDSM) lub modułom do routerów (NM-IDS);

- **zapobieganie atakom paraliżu usług (DDoS)** – oprócz prostych ataków sieciowych, dających się stosunkowo prosto wykryć, firmy coraz częściej stoją przed groźbą ataków paraliżu usług pochodzących z wielu źródeł rozproszonych w internecie. Identyfikacja takich ataków i skuteczne zapobieganie wymaga zaawansowanej analizy statystycznej ruchu w sieci, z uwzględnieniem wielu jego parametrów. Analiza i identyfikacja to pierwszy krok, na podstawie wniosków należy następnie uruchomić mechanizmy blokujące takie ataki. Cisco Guard jest nowatorskim systemem analizy ruchu pozwalającym na dynamiczne filtrowanie ruchu eliminujące nawet do 99 proc. ruchu niepożądanego, pochodzącego np. z ataków DDoS na firmowe serwery DNS. Takie rozwiązanie zastosowane przez operatora pozwoli na uniknięcie przeciążenia łącza dostępowego i zapewnienie widoczności np. sklepu internetowego przez swoich klientów pomimo ataku;
- **monitorowanie i zarządzanie** – żadne z mechanizmów nie będą skuteczne, jeżeli administrator nie ma żadnego wglądu w to, co się dzieje w jego sieci. Administrator powinien zbierać dane wystarczające do tego, by znać stan normalny swojej sieci i móc szybko identyfikować anomalie zgłaszane przez urządzenia oraz obserwować reakcje posiadanych systemów zabezpieczeń. Bez zbierania tych danych, a przede wszystkim bez inteligentnego systemu decydującego, które z milionów wydarzeń należy przedstawić w przejrzystej formie, panowanie nad siecią staje się niemożliwe po przekroczeniu pewnej liczby urządzeń. Przykładem kompleksowego systemu pozwalającego zbierać i analizować dane z szeregu źródeł (firewalle, routery, przełączniki, sondy IDS itp.) jest Cisco Security Monitoring, Analysis and Response System (CS-MARS).

Wszystkie te elementy z osobna podnoszą bezpieczeństwo sieci, jednak same urządzenia i technologie to nie wszystko. Potrzebna jest wizja, koncepcja, architektura zapewniająca współpracę tych elementów. Firma Cisco od lat promuje bezpieczeństwo, począwszy od publikacji zaleceń (architektura SAFE), poprzez dostępną od 2004 roku architekturę kontroli dostępu do sieci (NAC – *Network Access Control*), w ramach której współpracują ze sobą czołowi producenci zabezpieczeń (np. Microsoft, Network Associates, Symantec, Trend Micro, czy IBM), aż po ogłoszony w tym roku kolejny etap tej architektury, czyli adaptatywną reakcję sieci na zagrożenia (Adaptive Threat Defense). Są to konsekwentnie realizowane kroki zainicjowanej przez Cisco koncepcji Self-Defending Network, czyli samobroniącej się sieci.

Marek Moskal
inżynier systemowy w Cisco Systems

Lepiej zapobiegać niż leczyć

Firma Cisco Systems poinformowała o wprowadzeniu na rynek nowej serii produktów pod nazwą Cisco Adaptive Security Appliance (ASA) 5500, obejmującej nowatorskie, wielofunkcyjne urządzenia umożliwiające profilaktyczną ochronę sieci przed atakami.

Urządzenia z serii Cisco ASA 5500 kontrolują ruch w sieci (w tym ruch generowany przez aplikacje) i zapewniają elastyczną łączność w wirtualnych sieciach prywatnych (VPN), a przy tym pozwalają obniżyć łączne koszty wdrożenia i eksploatacji zabezpieczeń oraz uprościć ich strukturę.

Seria Cisco ASA 5500, która obejmuje modele Cisco ASA 5510, Cisco ASA 5520 oraz Cisco ASA 5540, jest kluczowym elementem rozpoczętego niedawno programu adaptacyjnej obrony przed zagrożeniami (*Adaptive Threat Defense*). Program ten stanowi kolejną fazę realizacji strategii zabezpieczeń *Self-Defending Network, (SDN*) Cisco. Wszystkie urządzenia z nowej serii zaprojektowano w taki sposób, aby zapewnić ochronę małych, średnich oraz dużych przedsiębiorstw, a przy tym umożliwić skalowanie pod względem liczby jednocześnie świadczonych usług oraz ujednolicenie zarządzania. Dzięki temu urządzenia te pozwalają jednocześnie korzystać z wielu usług ochrony z zachowaniem dużej wydajności i bez zwiększania złożoności eksploatacji.

W nowych rozwiązaniach wykorzystano wszechstronne, a zarazem zaawansowane zabezpieczenia stosowane wcześniej w wysokiej jakości urządzeniach zabezpieczających z serii PIX i IPS 4200 oraz koncentratorach VPN 3000. Ponadto produkty z serii ASA 5500 oferują rozbudowany zestaw usług sieci VPN, w tym zdalny dostęp z wykorzystaniem technologii IPSec i SSL, a także pozwalają realizować połączenia między ośrodkami w technologii IPSec, z zastosowaniem mechanizmów gwarantowania jakości usług (QoS). Dodatkowe zalety nowych produktów to duże możliwości integracji z sieciami IP oraz obsługa mechanizmów gwarantowania jakości usług (QoS), routingu, protokołu IPv6 oraz multicastingu. Dzięki temu opisywane urządzenia można instalować w sieciach bez zakłócania dozwolonego ruchu oraz przerywania pracy aplikacji.

– *Tradycyjny model wdrażania usług ochrony powoduje powstawanie hermetycznych grup urządzeń, a ponadto zmusza przedsiębiorstwa do kompromisów między efektywnością działania a wszechstronnością zabezpieczeń* – mówi **Joel Conover**, starszy analityk ds. infrastruktury przedsiębiorstw w firmie Current Analysis. – *Integracja wielu technologii w ramach urządzeń z serii ASA 5500 pozwala rozwiązać problem zarządzania licznymi urządzeniami zabezpieczającymi. Dzięki temu możliwe i opłacalne staje się wdrażanie wszechstronnych usług ochrony obejmujących większą liczbę lokalizacji sieciowych.*

Adaptacyjna obrona przed zagrożeniami

Urządzenia z serii Cisco ASA 5500 oferują zaawansowane usługi zapewniające adaptacyjną obronę przed zagrożeniami, w tym mechanizm Anti-X, zabezpieczenia aplikacji oraz funkcje kontroli sieci i powstrzymywania zagrożeń zaprojektowane w celu zapewnienia ujednoliconej, pełnej ochrony zasobów o znaczeniu krytycznym. Sieciowe mechanizmy obronne Anti-X chronią systemy klientów przed robakami i wirusami oraz programami typu spyware i adware, a także pozwalają precyzyjnie kontrolować ruch w sieci, zapobiegać atakom hakerów i włamaniom oraz bronić się przed atakami polegającymi na odmowie usługi (DoS). Jednocześnie korelacja wszystkich zdarzeń związanych z zabezpieczeniami odbywa się w ramach jednego urządzenia.

Usługi ochrony aplikacji dostępne w urządzeniach z serii Cisco ASA 5500 umożliwiają zaawansowaną kontrolę aplikacji oraz nadzór nad nimi, tym samym zapewniając dynamiczną i niezawodną ochronę aplikacji działających w sieci. Powyższe usługi obejmują nadzór nad silnie obciążającymi sieć programami typu P2P, takimi jak Kazaa czy programy do natychmiastowego przesyłania wiadomości (komunikatory), a także kontrolę adresów URL w sieci WWW oraz ochronę i sprawdzanie integralności podstawowych aplikacji przedsiębiorstw (takich jak bazy danych). Dodatkowo dostępne są liczne mechanizmy ochrony dostosowane do potrzeb poszczególnych aplikacji w zakresie łączności Voice over IP (VoIP) oraz usług multimedialnych.

Kolejną funkcją urządzeń z serii Cisco ASA 5500 są usługi sterowania siecią i powstrzymywania zagrożeń, które zapewniają precyzyjny nadzór nad użytkownikami, dostępem do aplikacji i przepływem ruchu w sieci, a także ich segmentację. Obejmują one zaporę z mechanizmem kontroli pakietów warstw 2–4, która pozwala klientom monitorować stan wszystkich połączeń w sieci, a tym samym uniemożliwić nieupoważnionym osobom dostęp do niej. Produkty z serii Cisco ASA 5500 oferują także funkcje wirtualizacji, które umożliwiają segmentację sieci oraz zapewniają skalowalność usług.

Zaawansowana ochrona dostępu do sieci VPN

Produkty z serii ASA 5500 oferują obszerny zestaw usług umożliwiających tworzenie sieci VPN w oparciu o technologie IPSec i SSL. Usługi te można integrować z opisanymi powyżej technologiami adaptacyjnej obrony przed zagrożeniami, aby uniemożliwić wykorzystanie sieci VPN do przesyłania robaków i wirusów oraz dokonywania włamań. Dzięki konwergencji mechanizmów obsługi sieci VPN w technologii IPSec i SSL, urządzenia z serii Cisco ASA 5500 można stosować w dowolnych wariantach instalacji sieci VPN. Obejmują one sieci łączące ośrodki, zarządzane komputery, pełny lub ograniczony dostęp do sieci przedsiębiorstwa oraz dostęp do sieci partnerów bądź ekstranetu. Klienci mogą zapewnić bezpieczny dostęp zdalny dowolnym użytkownikom, niezależnie od miejsca ich pobytu, w oparciu o jedno urządzenie i jedną infrastrukturę zarządzania. Urządzenia z serii Cisco ASA 5500 można również integrować z dotychczasowymi klastrami koncentratorów Cisco VPN 3000. W ten sposób klienci mogą wykorzystać dotychczasowe inwestycje w sieci VPN, a zarazem wdrożyć najbardziej zaawansowane mechanizmy obsługi tych sieci oraz zabezpieczenia.

Oszczędna i funkcjonalna platforma

Rozwiązania z serii Cisco ASA 5500 pozwalają zwiększyć opłacalność i efektywność działania systemów zabezpieczeń wdrażanych przez klientów. Umożliwiają one między innymi rozszerzanie usług w oparciu o moduły programowe i sprzętowe, standaryzację platform obejmujących wiele lokalizacji, uproszczenie eksploatacji poprzez wdrożenie wspólnej usługi zarządzania i monitorowania obejmującej wiele urządzeń zabezpieczających oraz uproszczenie rozwiązywania problemów i lokalizowania usterek. Profil usług umożliwia dostosowywanie rozwiązań do potrzeb poszczególnych lokalizacji i funkcji. Dzięki temu klienci mogą tworzyć w oparciu o urządzenia Cisco ASA 5500 standardowe systemy zabezpieczeń wykorzystywane przez wielu użytkowników, unikając stosowania wielu niezgodnych ze sobą platform oraz struktur zarządzania. Metoda adaptacyjna polegająca na wykorzystaniu jednego urządzenia do realizacji wielu usług pozwala zmniejszyć liczbę wdrażanych (i wymagających zarządzania) platform oraz stworzyć wspólne środowisko do eksploatacji wszystkich wdrożonych rozwiązań i zarządzania nimi. Powyższa metoda pozwala uprościć konfigurowanie, monitorowanie, rozwiązywanie problemów oraz szkolenie personelu odpowiedzialnego za zabezpieczenia.

Wiele z ujednoliconych usług zarządzania dostępnych na platformie Cisco ASA 5500 jest świadczonych za pomocą modułu Adaptive Security Device Manager, który zapewnia zarządzanie pojedynczymi urządzeniami, oraz pakietu Cisco Security Management Suite, który umożliwia zarządzanie wieloma urządzeniami. Adaptive Security Device Manager to zintegrowany menedżer urządzeń działający w oparciu o sieć WWW, umożliwiający konfigurowanie wszystkich urządzeń zabezpieczających oraz urządzeń sieci VPN. Oferuje on także funkcje zintegrowanego monitorowania stanu i usług oraz raportowania w tym zakresie; rozwiązanie to jest przeznaczone do obsługi mniejszych instalacji, obejmujących maksymalnie 10 urządzeń.

Pakiet Cisco Management Security Suite stworzono natomiast z myślą o większych instalacjach. Umożliwia on zarządzanie wieloma usługami, funkcjami i ośrodkami na podstawie reguł. Pakiet ten można stosować w środowiskach platform hybrydowych, w ramach których funkcjonują różne urządzenia, routery i przełączniki. Dodatkowo obejmuje on mechanizmy nadzoru nad aktualizacją oraz kontroli obejmujące wielu użytkowników i całe działy. Połączenie wszystkich powyższych funkcji zarządzania umożliwia klientowi zaawansowane administrowanie pojedynczymi urządzeniami oraz grupami konwergentnych urządzeń zabezpieczających.

Wszechstronne usługi ochrony

Klienci używający urządzeń z serii Cisco ASA 5500 (a także wszelkich zabezpieczeń oferowanych przez Cisco) mogą korzystać z usług Cisco Incident Readiness and Response Services, które umożliwiają ocenę bieżącej gotowości zabezpieczeń. Ponadto dostępne są procesy i procedury projektowania zabezpieczeń pozwalające wykrywać, neutralizować i minimalizować ataki w sieci. Pod koniec maja Cisco udostępni również bezpłatny pakiet zasobów MySDN, dostępny w sieci WWW, który obejmuje informacje na temat słabych punktów, aktualnych zagrożeń, sygnatur oraz strategii neutralizowania zagrożeń. Nowe usługi wchodzą w zakres oferty zabezpieczeń Cisco obejmującej cały cykl eksploatacji produktów. Połączenie tych rozwiązań zapewnia ochronę sieci na poziomie całego systemu.

Opracowano na podstawie materiałów firmy Cisco Systems

Urządzenia pod nadzorem

Firma Cisco Systems przedstawiła urządzenie Cisco Wireless Location Appliance 2700, które jest pierwszym w branży, łatwym do wdrożenia rozwiązaniem umożliwiającym jednoczesne monitorowanie tysięcy bezprzewodowych urządzeń klienckich zgodnych ze standardem IEEE 802.11 w ramach dotychczasowych infrastruktur bezprzewodowych sieci lokalnych (WLAN) klientów. Cisco Wireless Location Appliance 2700 umożliwia ekonomiczne, precyzyjne lokalizowanie urządzeń w bezprzewodowych sieciach lokalnych, co pozwala na optymalizację przesyłania głosu, danych.

Dodatkową zaletą urządzenia jest możliwość szybkiego rozpoznawania zagrożeń. Ponadto można je ściśle zintegrować z rozwiązaniami technicznymi i aplikacjami oferowanymi przez innych partnerów. Dzięki temu można sprawniej tworzyć nowe, ważne aplikacje dla przedsiębiorstw w celu optymalizacji wykorzystania zasobów oraz usprawnienia procesów biznesowych.

W urządzeniu Cisco Wireless Location Appliance 2700 zastosowano mechanizm identyfikacji radiowej oferowany przez system sterowania bezprzewodowego Cisco WCS (*Wireless Control System*). Umożliwia on lokalizowanie urządzeń korzystających z sieci zgodnych ze standardem 802.11 (zarówno upoważnionych, jak i nieupoważnionych) z dokładnością do kilku metrów. Można w ten sposób określać położenie laptopów, komputerów kieszonkowych, zestawów słuchawkowych w technologii Voice over Wireless LAN (VoWLAN), nielegalnych punktów dostępowych oraz urządzeń wyposażonych w aktywne znaczniki identyfikacji radiowej (RFID) zgodne ze standardem 802.11. Położenie każdego urządzenia jest nanoszone w trybie graficznym na plany budynków w systemie Cisco WCS, co umożliwia administratorom sieci szybkie i łatwe ich odnajdywanie.

Firma IBM, globalny partner strategiczny Cisco, stworzyła jednolitą infrastrukturę bezprzewodowej sieci lokalnej umożliwiającą realizację całej gamy usług, w oparciu o którą tworzone są nowe aplikacje bezprzewodowe przeznaczone dla klientów z różnych sektorów rynku (w tym w zakresie usług lokalizacyjnych).

– *Usługi lokalizacyjne umożliwiają przedsiębiorstwom wdrażanie nowych aplikacji pozwalających wykorzystać wyjątkowe możliwości, jakie stwarza łączność bezprzewodowa* – uważa **Don Lopes**, dyrektor ds. rozwoju globalnego rynku łączności bezprzewodowej w IBM Global Services. – *Po zintegrowaniu z systemem bezprzewodowej sieci lokalnej usługi lokalizacyjne stają się ważnym elementem eksploatacji i ochrony sieci, a także zarządzania nią.*

Cisco i IBM wspólnie promują wykorzystanie aktywnych znaczników identyfikacji radiowej (RFID) w bezprzewodowych sieciach lokalnych. Znaczniki te pozwalają klientom, takim jak Westchester Medical Center, monitorować cenne urządzenia przenośne i urządzenia zgodne ze standardem 802.11 oraz zarządzać nimi.

– *W ośrodku Westchester Medical Center obsługa klienta ma kluczowe znaczenie* – twierdzi **Tom Toscano**, dyrektor ds. telekomunikacyjnych w ośrodku Westchester Medical Center. – *Urządzenie lokalizacyjne oferowane przez Cisco i IBM pozwala nam precyzyjnie określać miejsce przechowywania poszczególnych elementów wyposażenia szpitala – od wózków inwalidzkich po aparaturę EKG – dzięki czemu nasi pracownicy mogą zapewnić najlepszą i najszybszą opiekę.*

Urządzenie Cisco Wireless Location Appliance 2700 umożliwia wdrożenie różnych aplikacji wykorzystujących zalety łączności bezprzewodowej, które umożliwiają między innymi:

- ✔ monitorowanie zasobów – w tym zapobieganie zgubieniu bądź kradzieży cennych urządzeń bezprzewodowych, takich jak nowoczesna aparatura medyczna, a także szybkie lokalizowanie najważniejszych pracowników i zasobów w obrębie całego przedsiębiorstwa korzystającego z łączności bezprzewodowej;
- ✔ zarządzanie zasobami i automatyzacja przepływu pracy – w tym optymalizację wykorzystania zasobów oraz usprawnienie przepływu i rozdziału pracy;
- ✔ ochronę – poprzez lokalizowanie źródeł zagrożeń w bezprzewodowej sieci lokalnej, takich jak nielegalne punkty dostępowe i urządzenia, w celu sprawnego rozwiązywania problemów;
- ✔ wykorzystanie usług przesyłania głosu w bezprzewodowych sieciach lokalnych (*Voice over Wireless LAN*) – w tym precyzyjne lokalizowanie urządzeń w celu zapewnienia zgodności z wymaganiami w tym zakresie, obejmującymi na przykład rozszerzone usługi służb ratunkowych.

– *Urządzenie Cisco Wireless Location Appliance pozwala precyzyjnie lokalizować urządzenia na potrzeby aplikacji o znaczeniu krytycznym* – mówi **Alan Cohen**, dyrektor ds. produktów w dziale sieci bezprzewodo-

wych Cisco. – *Współpracując z wieloma różnymi partnerami dostarczającymi rozwiązania techniczne i aplikacje, Cisco stara się promować usługi lokalizacyjne jako nieodzowny element wszystkich bezprzewodowych sieci lokalnych.*

Wraz z urządzeniem Cisco Wireless Location Appliance oferowany jest obszerny, otwarty interfejs programowania, który ułatwia wdrażanie usług lokalizacyjnych w przedsiębiorstwach. Interfejs ten służy do ścisłej integracji z zewnętrznymi aplikacjami, w tym rozwiązaniami do monitorowania urządzeń bezprzewodowych w sieciach 802.11 firmy PanGo Networks. Firma PanGo – jeden z największych dostawców aplikacji lokalizacyjnych – zintegrowała oferowane rozwiązanie do identyfikacji radiowej w sieciach Wi-Fi, PanGo Locator, z urządzeniem Cisco Wireless Location Appliance. Ścisła integracja aplikacji PanGo Locator z urządzeniem umożliwia prezentację zasobów w środowisku bezprzewodowej sieci LAN w czasie rzeczywistym. Oferowane rozwiązanie pozwala znacznie lepiej wykorzystać krytyczne zasoby, takie jak wózki inwalidzkie i pompy infuzyjne w placówkach służby zdrowia lub wózki widłowe i palety w zakładach produkcyjnych. Tym samym umożliwia obniżenie kosztów inwestycyjnych i kosztów leasingu, a także przyspiesza wyszukiwanie urządzeń oraz zapewnia sprawniejszą obsługę ze strony personelu.

– *Informacja o nowym rozwiązaniu to doskonała wiadomość dla każdego klienta, który chce zwiększyć możliwości posiadanej sieci oraz zarządzać nią w inteligentny sposób* – stwierdza **Mike McGuinness**, prezes i dyrektor generalny firmy PanGo Networks. – *Cisco umożliwiło bezproblemową integrację aplikacji lokalizacyjnych, takich jak PanGo Locator, z sieciami, a tym samym tworzenie rozwiązań o możliwościach znacznie wykraczających poza dostępne dotychczas na rynku.*

W celu zapewnienia klientom ochrony inwestycji w bezprzewodowe sieci lokalne i umożliwienia ich dalszej rozbudowy Cisco będzie udostępniać kolejne usługi lokalizacyjne w ramach dodatkowych aplikacji zewnętrznych.

– *Bardzo nas cieszy wprowadzenie przez Cisco nowatorskiego i wszechstronnego urządzenia Wireless Location Appliance. Jest ono pierwszym w branży rozwiązaniem umożliwiającym rozpoznawanie lokalizacji infrastruktury w bezprzewodowych sieciach lokalnych i stanowi solidną podstawę do tworzenia różnorodnych aplikacji lokalizacyjnych. Ponadto zapewnia klientom obniżenie kosztów eksploatacji sieci* – konkluduje **Yuval Bar-Gil**, dyrektor generalny firmy AeroScout. – *Współpracujemy z Cisco, aby zapewnić ścisłą integrację urządzenia Cisco Wireless Location Appliance z aplikacją AeroScout MobileView, która służy do monitorowania systemów przedsiębiorstwa. Pozwoli to stworzyć całościowe rozwiązanie dla klientów.*

Opracowano na podstawie materiałów Cisco Systems

Łatwiejsze zarządzanie i większa dostępność

Unisys zaprezentował serwer ES7000 540, wyposażony w procesory Intel Xeon oraz udoskonalony system zarządzania Sentinel. Dodatkowo firma udostępniła dane dowodzące, iż serwery ES7000, działając na platformie Wintel, w pełni dorównują sprawnością systemom Unix/RISC.

Prowadzone przez dwa lata badania wielu systemów eksploatowanych przez klientów firmy Unisys pokazują, iż 75 proc. serwerów ES7000 osiągnęło wskaźnik dostępności przekraczający 99,999 proc. Co więcej, system Sentinel umożliwia zredukowanie liczby osób administrujących system nawet o 40 proc.

Dyspozycyjność na poziomie przewyższającym 99,999 proc.

W pierwszym udostępnionym raporcie dotyczącym dyspozycyjności serwerów pracujących w rzeczywistych środowiskach biznesowych pod kontrolą systemu Windows firma Unisys stwierdziła, że 78 proc. spośród badanych systemów osiągnęło pełną dyspozycyjność, pracując non stop, bez żadnych przestojów. Ogólnie, serwery pracujące pod kontrolą Windows 2000 Datacenter Server lub Windows Server 2003 Datacenter Edition osiągnęły średni stopień dostępności na poziomie 99,996 proc. Dane do raportu gromadzone były na przestrzeni dwóch lat i pochodziły z rzeczywistych środowisk produkcyjnych klientów – użytkowników serwerów ES7000 na terenie Ameryki Północnej. Uzyska ne wyniki dotyczą konfiguracji nieklastrowych. Nie są w nich uwzględnione przestoje planowane, np. związane z procedurami konserwacyjnymi. Unisys osiągnął taki rezultat bez implementacji kosztownych rozwiązań instalowanych na wypadek awarii. Szczegóły raportu dostępne są pod adresem: www.unisys.com/datacenter/availability-study/.

Enterprise Server ES7000 – seria Aries

– *Serwer ES7000 oferuje nam wydajność, jakiej potrzebujemy, pracując w środowisku, które jest bardzo elastyczne, łatwe w zarządzaniu, skalowalne i pozwala zminimalizować nieplanowane przestoje* – mówi **Gary Clark**, dyrektor korporacyjnego oddziału usług informatycznych La-Z-Boy. – *Dzięki intensywnym testom zauważyliśmy, że ES7000 pracuje z dyspozycyjnością rzędu pięciu dziewiątek. Chociaż początkowo zaangażowaliśmy ES7000 w projekt konsolidacji 12 serwerów aplikacji i baz danych, wydajność skalowała się tak dobrze i była tak wiarygodna, iż obecnie uruchamiamy więcej niż 80 baz danych na jednej 8-procesorowej partycji, znacząco ograniczając koszty związane z zakupem dodatkowego sprzętu.*

Większa wydajność przy mniejszej cenie, łatwiejsze administrowanie i niemal 100 proc. dyspozycyjność powodują, że Unisys ES7000 przyciąga klientów chętnych do czerpania korzyści z przejścia na systemy standaryzowane. To odpowiednia platforma dla kierownictwa, chcącego osiągnąć przewagę konkurencyjną poprzez obniżenie kosztów wynikających z zastosowania infrastruktury informatycznej standardu Windows. Obecnie z platformy ES7000 korzystają firmy na całym świecie. Wśród najnowszych klientów, którzy zdecydowali się na zakup platformy ES7000 są: SafeCo Insurance, Pier 1 Imports, State of Indiana, NTT Data of Japan, Kaufmannische Krankenkasse (KKH), czwarta pod względem wielkości firma oferujące ubezpieczenia zdrowotne na rynku niemieckim, władze Sztokholmu oraz Jungheinrich AG, niemiecka firma produkcyjna.

– *Wyniki naszego raportu dotyczącego dyspozycyjności pokazują, że Windows jest nie tylko systemem klasy enterprise, ale faktycznie stanowi najlepszą opcję dla klientów, którym zależy na optymalizacji budżetu IT swojej firmy* – twierdzi **Dennis Oldroyd**, dyrektor ds. serwerów w Microsoft. – *Unisys ES7000 razem z Windows Datacenter Edition wyraźnie pokazał, iż oferuje niemal 100-proc. niezawodność. Korzyści finansowe*

płynące z użytkowania tych technologii stanowią obecnie nieodpartą alternatywę.

– Wyniki badań, jakie przeprowadził Unisys, są imponujące – mówi **Richard Dracott**, odpowiedzialny za Enterprise Marketing and Planning w Grupie Enterprise Platforms w firmie Intel. *– ES7000 oparty na procesorach Intel Xeon oraz wykorzystujący technologię firmy Microsoft zaprezentował niesłychany poziom dostępności w rzeczywistym środowisku biznesowym. To wyraźnie pokazuje, że klienci mogą osiągać znaczącą wydajność, równocześnie czerpiąc korzyści z tych standardowych technologii.*

Administrowanie przy użyciu technologii Sentinel

Oprogramowanie Sentinel daje serwerowi ES7000 zaawansowane możliwości, przez co stanowi on odpowiednią platformę dla realizacji krytycznych zadań biznesowych. W przeciwieństwie do konkurencji, oferującej systemy ogólnego monitorowania i raportowania, Sentinel automatycznie wykrywa problemy serwera, systemu operacyjnego, jak również aplikacji i baz danych, rozwiązując je bez ingerencji człowieka. Unisys oferuje narzędzia do zarządzania aplikacjami, takimi jak Microsoft SQL Server, co daje najlepszą w swojej klasie wydajność, niezawodność i łatwość administrowania.

– Pierwsi doceniliśmy potencjał, jaki Windows może mieć w kategorii systemów produkcyjnych i nadal podkreślamy nasze pierwszeństwo w tej dziedzinie – uważa **Chander Khanna**, wiceprezes zajmujący się marketingiem platform w Unisys Corp. *– Jesteśmy zobowiązani do tego, aby nasi klienci osiągali ekonomiczne korzyści, stosując centra przetwarzania danych w standardzie Windows. Determinacja użytkowników ES7000 pokazuje korzyści płynące ze standaryzacji platform produkcyjnych Microsoft/Intel.*

Najlepsza dyspozycyjność wśród systemów produkcyjnych

32-procesorowy serwer Unisys ES7000 540 (Orion) poddany badaniu TPC wykonał 304,148.50 transakcji w ciągu minuty (tpmC), przy cenie 6,18 dolarów za jedną transakcję. Według TPC (*Transaction Processing Council*), ES7000 jest najbardziej wydajnym serwerem spośród maszyn 32-bitowych.

Poddawany testom serwer był wyposażony w 32 procesory Intel Xeon MP, o częstotliwości pracy 3 GHz każdy, 4 MB pamięci podręcznej 3. poziomu oraz 64 GB pamięci operacyjnej. Serwer obsługiwał Microsoft SQL Server 2000 Enterprise Edition i pracował w oparciu o system operacyjny Microsoft Windows Server 2003 Datacenter Edition. Test TPC-C jest standardowym testem pomiaru wydajności transakcyjnej i ekonomicznej (mierzy stosunek ceny do wydajności) serwerów.

3D – Visible Enterprise (3D-VE)

Strategia 3D-VE łączy procesy biznesowe z infrastrukturą informatyczną. Uwidacznia związki przyczynowo-skutkowe, jakie zachodzą pomiędzy procesami biznesowymi a wykorzystywanymi rozwiązaniami technologicznymi. Pozwala przewidzieć skutki potencjalnych decyzji biznesowych, zanim decyzje te zostaną podjęte, a pieniądze wydane. Serwer ES7000 daje organizacjom elastyczność i bezpieczeństwo niezbędne do zagwarantowania, że posiadana infrastruktura informatyczna sprosta ich celom biznesowym.

Enterprise Server ES7000 – seria Aries

Przy współpracy z Microsoft, Unisys przedstawił architekturę IB for MSA (*Infrastructure Blueprint for Microsoft Systems Architecture*). IB for MSA jest w pełni sprawdzoną, udokumentowaną architekturą, bazującą na najlepszych praktykach wykorzystywanych przez wiodących na rynku dostawców technologii, w tym firmę Unisys. Daje to klientom gwarancję, że Unisys rozumie ich potrzeby w zakresie infrastruktury i może dostarczyć im całościowe rozwiązania, pozwalające osiągać zamierzone cele biznesowe.

Wysoka dostępność gwarantowana przez serwer ES7000 stanowi fundament architektury IB for MSA, która, z kolei, opisuje kroki, jakie należy podjąć przy budowie centrum przetwarzania danych na platformie Windows. IB for MSA mówi, jak zagwarantować wysoką dostępność całej infrastruktury. Dotyczy to również poawaryjnego odtwarzania danych, będącego kluczowym elementem strategii 3D-VE.

Opracowano na podstawie materiałów firmy Unisys

Niniejszy artykuł ukazał się w INFOTELU NR 6/2004

System routujący CRS 1

Niedawno Cisco Systems zaprezentowało nowy router, a właściwie system routujący – Carrier Routing System 1 (CRS-1), nad którym firma pracowała przez ponad pięć lat. Jest to pierwszy router zbudowany z myślą o rytmie pracy analogicznym do central telefonicznych – raz włączony ma pracować przez dziesięciolecia bez przerw konserwacyjnych mimo kolejnych uaktualnień funkcjonalności oraz rozbudowy pojemności. I praktycznie bez przerw spowodowanych przez awarie.

Nowatorska architektura systemu minimalizuje skutki zarówno awarii sprzętu, błędów oprogramowania, jak i niektórych typów ataków hakerskich, umożliwia też zapewnienie ciągłości pracy na poziomie 99,999 proc. Oznacza to przestoje krótsze niż 5 minut w ciągu roku.

Już w wersji podstawowej przepustowość systemu – 1,2 Tbit/s – wystarczyłaby do udostępnienia ponad dwu milionom mieszkańców Warszawy osobistych łączy o przepustowości 0,5 Mbit/s. W wersji najbardziej rozbudowanej pojemność systemu wyposażonego w 1152 karty 40 Gbit/s wynosi 92 Tbit/s. To o dwa rzędy wielkości więcej niż jakikolwiek dzisiejszy router. Dwa takie systemy wystarczyłyby do zapewnienia równoczesnej łączności telefonicznej wszystkim mieszkańcom Ziemi. Rzeczywistym przeznaczeniem tych routerów jest jednak uproszczenie budowy operatorskich punktów dostępu do sieci (*Point Of Presence*) oraz obniżenie kosztów ich eksploatacji.

Nowatorskie podejście do punktów dostępu

Dzisiejsze punkty dostępu zawierają kilka rodzajów urządzeń: routery dostępowe służące do podłączania klientów i obsługujące zaawansowane usługi operatorskie (takie, jak np. MPLS czy QoS), urządzenia agregujące ruch, routery szkieletowe, których zadaniem jest szybkie przełączanie dużej ilości ruchu pomiędzy urządzeniami brzegowymi, a także połączenie POP z siecią szkieletową operatora. Do tego dochodzą urządzenia realizujące specyficzne funkcje – np. cache, rozwiązania bezpieczeństwa sieciowego itp. Problem polega na tym, że ze względu na liczbę niezbędnych urządzeń – dodatkowo zdublowanych ze względu na wymagany poziom niezawodności – 20-40 proc. wszystkich portów w urządzeniach jest wykorzystywanych wewnętrznie, do budowy struktury samego POP.

CRS-1, dzięki swojej niezawodności i wydajności, może zastąpić większość tych urządzeń radykalnie zmniejszając zarówno liczbę potrzebnych połączeń, jak i upraszczając zarządzanie. Nie oznacza to bynajmniej konieczności wyrzucenia starych urządzeń szkieletowych. Od wielu lat w budowie sieci operatorskich obowiązuje reguła „Dzisiejszy szkielet jest brzegiem jutra" – w miarę upływu czasu rośnie liczba typów interfejsów do istniejących urządzeń szkieletowych oraz liczba dostępnych funkcji oprogramowania. Dzięki temu stare urządzenia szkieletowe po odpowiednim przekonfigurowaniu mogą zostać przeniesione na brzeg sieci i wykorzystane do podłączania klientów. Tak stało się z routerami z serii 7xxx – pierwotnie skonstruowanymi z myślą o szkielecie sieci, a następnie przeniesionymi na jej brzeg. Tak stanie się też z routerami Cisco 12000 GSR już dziś zresztą wiele z nich jest wykorzystywanych na brzegu sieci.

Architektura wzorem z superkomputerów

CRS-1 wykorzystuje całkowicie nową, rozproszoną architekturę sprzętową wzorowaną na architekturze

superkomputerów. W najprostszej wersji cały system mieści się w pojedynczej, wolno stojącej szafie. Maksymalnie rozbudowany system obejmuje 72 stelaże zawierające karty liniowe oraz osiem stelaży z rozproszoną, trzystopniową matrycą przełączającą opartą na polach komutacyjnych Beneša. Oczywiście, rozbudowę o kolejne stelaże można wykonać bez przerywania obsługi już podłączonych abonentów.

Stelaż z kartami liniowymi zawiera umieszczoną centralnie pasywną magistralę (tzw. midplane), do której od tyłu włączane są karty liniowe o przepustowości 40 Gbit/s każda, natomiast od przodu – moduły interfejsów. Dzięki takiej konstrukcji zmiana typu łącza nie wymaga wymiany całej karty liniowej, a jedynie modułu interfejsów – analogicznie do wymiany modułów optycznych GBIC w urządzeniach gigabitowych.

Obecnie karta liniowa może współpracować także z modułem OC-768/STM-256 o przepustowości 40 Gbit/s, czteroportowym modułem OC-192/STM-64 (4x10 Gbit/s) albo cztero- lub ośmioportowym modułem 10 GbE. W tym ostatnim przypadku występuje nadsubskrypcja, bardzo często bowiem umowa usługowa przewiduje ograniczenie gwarantowanego pasma (np. CIR) w stosunku do teoretycznej przepustowości łącza; w takich przypadkach nadsubskrypcja umożliwia lepsze wykorzystanie szkieletu. W przyszłości, w miarę wzrostu potrzeb użytkowników, będzie również wzrastała różnorodność kart interfejsów.

Każda karta liniowa zawiera dwa układy SPP (*Silicon Packet Processor*), z których jeden obsługuje 8 tys. kolejek wejściowych, a drugi – 8 tys. kolejek wyjściowych. Liczba kolejek będzie mogła być w przyszłości dodatkowo zwiększona. Wbrew nazwie, opracowany wspólnie z firmą IBM układ SPP jest nie tyle procesorem, ile macierzą pracujących równolegle 32-bitowych procesorów RISC o łącznej wydajności 44 GIPS (gigainstrukcji na sekundę), a więc kilkakrotnie więcej od najszybszych procesorów Intela i AMD. Ten specjalizowany układ komunikacyjny zawiera w sumie 185 milionów tranzystorów (ponad trzykrotnie więcej niż Pentium 4 Intela i prawie o połowę więcej niż Prescott) i 38 milionów bramek. Jest to najbardziej skomplikowany ASIC (układ scalony specjalizowany do wykonywania określonego zadania) na świecie.

Oprogramowanie sterujące

Choć oprogramowanie sterujące pracą CRS-1 nosi nazwę Cisco IOS XR i ma interfejs użytkownika bardzo podobny do tradycyjnego IOS-a, nie ma z nim wiele wspólnego. W przeciwieństwie do „monolitycznego" poprzednika (przynajmniej z punktu widzenia użytkownika; wewnętrznie niektóre wersje systemu wprowadzały pewne elementy modularności), nowy system operacyjny jest oparty na mikrokernelu systemu czasu rzeczywistego QNX. Mikrojądro systemu wykonuje tylko najbardziej podstawowe funkcje związane z obsługą wątków oraz zarządzaniem i ochroną zasobów, m.in. pamięci, natomiast wszystkie pozostałe funkcje zostały przeniesione do procesów usługowych. Dzięki temu błędy w pracy procesów obsługujących nawet kluczowe funkcje systemu są natychmiast izolowane, a system jest bardzo wydajny i stabilny. Jest to jeden z pierwszych wypadków zastosowania tak radykalnego podejścia do oprogramowania sterującego pracą routerów. Dotychczasowe „modularne" systemy routerowe umożliwiają uruchamianie zaledwie od kilku do kilkunastu osobnych procesów, w IOS XR jest ich kilkaset.

Każda karta liniowa oraz zarządzająca wykonuje własną kopię mikrojądra, przy czym wzajemnie sprawdzają one swój stan i dostępność. Procesy usługowe mogą być wykonywane lokalnie lub na dowolnym procesorze zamontowanym w routerze. Taka architektura umożliwia niezależne zarządzanie procesami, uaktualnianie systemu oraz dodawanie

nowych funkcjonalności bez konieczności restartu całego systemu (*In-Service Software Upgrades*), a nawet bez wstrzymywania ruchu i utraty pakietów (*Non-Stop Forwarding*). Dzięki równoległej pracy poszczególnych elementów systemu, specjalnym procedurom kontrolnym włączonym we wszystkie kluczowe procesy, a także możliwości uruchamiania dowolnego procesu na dowolnym procesorze, w razie jakiejkolwiek awarii zadania realizowane przez uszkodzone zasoby mogą zostać wznowione na innych procesorach z zachowaniem stanu wszystkich sesji (*Stateful Switchover*). Cisco IOS XR wykorzystuje ponadto procedury samouzdrawiania oraz automatycznej obrony przed atakami DDoS (*Distributed Denial of Service*) kierowanymi przeciwko routerowi.

Ułatwione zarządzanie

Problemy ze stratą miejsca w rozrastających się punktach dostępu znane są od dawna. Dotychczasowe próby ich rozwiązania polegały na połączeniu routerów przy pomocy matrycy optycznej. Takie podejście umożliwia zaoszczędzenie portów abonenckich, jednak nie upraszcza zarządzania, które jest bardzo skomplikowane w przypadku dużych POP-ów. Tymczasem z punktu widzenia operatora CRS-1 jest pojedynczym węzłem sieci – bez względu na liczbę stelaży, z których się składa. Zdecydowanie upraszcza to zarządzanie zarówno samym systemem, jak i całą siecią. Efekt ten osiągnięto m.in. dzięki zastosowaniu specjalnych mechanizmów zbierających i agregujących wszelkie informacje pochodzące z różnych podzespołów urządzenia, a także wewnętrznych procedur odpowiedzialnych za rozesłanie wszelkich zmian konfiguracyjnych.

Nie zawsze jednak jeden wielki superrouter jest potrzebny. W wielu zastosowaniach przydatna jest możliwość przeznaczenia dedykowanego routera np. do obsługi VPN klienta. I z tym CRS-1 daje sobie radę. Jego oprogramowanie umożliwia partycjonowanie routera albo, innymi słowy, podział na routery wirtualne. Każdy taki router wirtualny jest całkowicie odseparowany logicznie od pozostałych – zawiera własny komplet wszystkich tablic, własne procesy obsługi, własne oprogramowanie, a nawet własną „przestrzeń adresową IP" (co jest istotne przede wszystkim w przypadku obsługi tzw. klas nierutowalnych, wykorzystywanych do obsługi sieci prywatnych).

Mnogość zastosowań

CRS-1 został skonstruowany jako urządzenie operatorskie mające obsługiwać usługi konwergentne – zarówno znane dzisiaj, jak i przyszłe. Internet w coraz większym stopniu przejmuje usługi dotychczas realizowane w niezależnych sieciach. Coraz większą popularność zdobywają łącza szerokopasmowe. W Japonii jest już ponad 11 mln abonentów usługi ADSL, a co kwartał przybywa kolejny milion. Kolejnych 2,6 mln abonentów korzysta z dostępu przez sieci telewizji kablowej, a 1,1 mln ze światłowodu do domu. W marcu tego roku całkowity ruch w dwóch największych japońskich węzłach internetowych przekroczył w sumie 100 Gbit/s. Podobną dynamikę obserwuje Deutche Telecom, który ma już ponad 4 mln abonentów DSL. Według firmy badawczej Point Topic's, pod koniec ub.r. było na świecie 73,4 mln abonentów samego tylko DSL.

Także w Polsce liczba abonentów sieci szerokopasmowych rośnie, choć nie tak szybko, jak można by oczekiwać. Pod koniec 2003 r. liczba użytkowników Neostrady wyniosła 177 tysięcy. Dla porównania: w tym samym czasie Aster miał ok. 34,6 tys. abonentów, a Chello (UPC) – 33 tys. Liczby te nie rzucają na kolana, jeżeli weźmie się pod uwagę, że Internet jest często postrzegany jako medium o znaczeniu cywilizacyjnym porównywalnym do bieżącej wody i kanalizacji. Być może jednak dzięki wykorzystaniu funduszy unijnych uda się przyspieszyć budowę nowoczesnej, szerokopasmowej sieci dostępowej, a to spowoduje wzrost zapotrzebowania na wydajne sieci szkieletowe. Ponadto w ostatnim czasie wszyscy trzej wspomniani operatorzy podnieśli przepustowości w ramach swoich pakietów usługowych o przynajmniej 30 proc., a niektórzy już przebąkują o usługach wideo na żądanie wymagających jeszcze większych prędkości – to również zwiększa obciążenie szkieletu. Nie tylko więc na świecie, ale i w Polsce będzie rosnąć rynek dla dużych urządzeń szkieletowych.

Zbudowanie CRS-1 ma dla Cisco Systems nie tylko znaczenie czysto handlowe. Urządzenie to bardzo wysoko „podnosi poprzeczkę" konkurentom. Przez długi czas wyglądało na to, że Cisco zapomniało o rozwoju technologii routingu, na której wyrosło, koncentrując się na inwestowaniu w takie rozwiązania, jak telefonia IP, bezpieczeństwo sieciowe czy sieci bezprzewodowe. Teraz firma pokazała „lwi pazur" również na tym polu. CRS jest też dla Cisco swego rodzaju „technologią kosmiczną". Doświadczenia zdobyte przy jego budowie już przenikają do sprzętu niższej klasy, a należy się spodziewać, że z biegiem czasu proces ten ulegnie znacznemu nasileniu.

(*Opracowano na podstawie materiałów firmy Cisco Systems*)

Niniejszy artykuł ukazał się w INFOTELU nr 10/2004

W pierwszej połowie sierpnia 2005 r. ukaże się następne wydanie z cyklu Biblioteka Infotela

BIBLIOTEKA INFOTELA

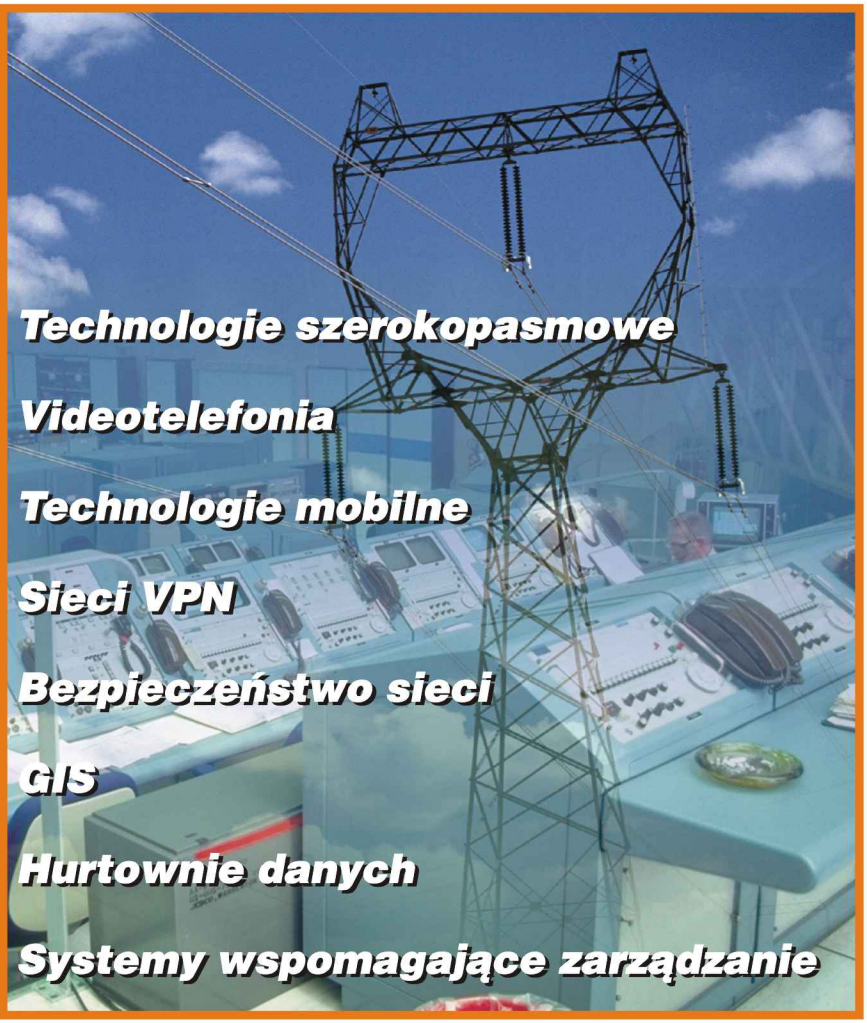
KOMUNIKACJA ELEKTRONICZNA DLA SŁUŻB MUNDUROWYCH

- Trankingowe systemy łączności
- Telefonia VoIP
- Systemy lokalizacyjne
- Urządzenia zasilające
- Radiotelefony i radiostacje
- Systemy transmisji danych
- Systemy dyspozytorskie
- Systemy szyfrowania danych

Na początku września 2005 r. ukaże się następne wydanie z cyklu Biblioteka Infotela

BIBLIOTEKA INFOTELA

KOMUNIKACJA ELEKTRONICZNA DLA ENERGETYKI



- Technologie szerokopasmowe
- Videotelefonia
- Technologie mobilne
- Sieci VPN
- Bezpieczeństwo sieci
- GIS
- Hurtownie danych
- Systemy wspomagające zarządzanie