



Centrální rozhraní sítí Krajského úřadu Vysočina - systémový projekt

verze 1.1

Vedoucí projektu:

Vladimír Končinský, Martin Matouš

Autoři dokumentu:

Pavel Sekanina, Petr Panáček,
P. Truneček, Petr Štěpánek,
Jiří Balda, Radim Koneček

Vytvořeno dne:

31. května 2004

ANECT a.s.

Vinohradská 112 • 130 00 Praha 3 • (+420) 271 100 100 • Česká republika
Videňská 125 • 619 00 Brno • (+420) 547 100 100 • Česká republika
Drieňová 34 • 821 02 Bratislava • (+421) 743 429 979 • Slovenská republika

Technické a obchodní informace uvedené v tomto dokumentu jsou výhradním majetkem ANECT a.s. a musí být proto drženy v tajnosti. Tento dokument je vytvořen výhradně pro účely systémového projektu centrálního rozhraní sítí pro Krajský úřad Vysočina, a proto tento materiál ani informace v něm obsažené nesmí být poskytnuty nebo vyzrazeny jiné straně nebo použity pro jakékoliv jiné účely bez předchozího písemně potvrzeného souhlasu společnosti ANECT a.s. a Krajského úřadu Vysočina

Projekt je vyhotoven písemně ve třech stejnopisech a elektronicky na jednom CD, z nichž jeden stejnopis a jedno CD si ponechá Krajský úřad Vysočina a dva ANECT a.s.

Záznamy o kontrole a změnách

Kontrola

Kontrola	Jméno	Funkce	Datum
Věcné správnosti	Pavel Sekanina	vedoucí oddělení Systémy a aplikace	31. 5. 2004
Elektronické verze	Kateřina Grofová	administrátorka	1. 6. 2004
Tištěné verze	Tereza Bursíková	administrátorka	1. 6. 2004

Změny

Datum	Jméno	Verze	Popis změny

Obsah:

Záznamy o kontrole a změnách.....	3
Obsah:	4
Seznam obrázků:	7
Seznam tabulek:.....	8
1. Zadání.....	1-1
2. Všeobecný přehled.....	2-1
2.1. Účel	2-1
2.2. Cíl systémového projektu	2-2
2.3. Vzájemné vazby v rozvoji informačních technologií	2-3
2.3.1. Cena komunikační infrastruktury	2-3
2.3.2. Kritické množství a kritický čas	2-3
2.3.3. Dostupnost telekomunikační infrastruktury	2-3
2.3.4. Informační vzdělanost	2-4
2.3.5. Moderní veřejné služby	2-5
2.3.6. Životní úroveň	2-6
2.3.7. Prostředí pro elektronické podnikání	2-6
2.3.8. Růst objemu a demonopolizace telekomunikačního trhu	2-6
2.3.9. Bezpečnost elektronických služeb	2-7
2.3.10. Negativní vazby.....	2-8
3. Komunikační infrastruktura - síťové prostředí	3-1
3.1. Technologie WAN sítě	3-1
3.1.1. Virtuální privátní síť.....	3-1
3.1.2. Volba technologie pro implementaci VPN v síti ROWANet.....	3-2
3.2. Výběr technologie pro rozlehlou síť ROWANet	3-13
3.3. Infrastruktura a topologie	3-14
3.3.1. Základní principy návrhu topologie WAN sítě ROWANet.....	3-14
3.3.2. Topologie páteřní sítě.....	3-15
3.3.3. Distribuční vrstva.....	3-18
3.3.4. Přístupová vrstva	3-20
3.3.5. Redundantní topologie	3-20
3.4. Přenosová infrastruktura WAN sítě ROWANet.....	3-23
3.4.1. Přehled komunikačních technologií	3-23
3.4.2. Volba přenosové infrastruktury pro ROWANet - shrnutí	3-29
3.4.3. Využití alternativních infrastruktur.....	3-30
3.5. Výběr komunikačního protokolu a adresní plán.....	3-30
3.5.1. IPv4 versus IPv6	3-31
3.5.2. Adresní plán	3-31
3.6. Směrování	3-33
3.7. Internet	3-35
3.7.1. Internetová konektivita	3-35
3.7.2. Distribuce Internetu	3-35
3.8. Integrace s ostatními sítěmi	3-37
3.8.1. GOVBONE.....	3-37
3.8.2. Metropolitní síť.....	3-39
4. Dohled a správa síťové infrastruktury, informačních systémů (IS)	4-1
4.1. Modely správy IS	4-1
4.1.1. ISO modelu	4-1
4.1.2. Telco model	4-2

4.1.3. FAB model	4-3
4.2. Systémy pro zajištění služeb – Service Assurance	4-3
4.2.1. Systém sledování dostupnosti a provozu v síti - performance management	4-3
4.3. Systém správy chybových stavů sítě – fault management	4-4
4.4. Sledování služeb	4-6
4.4.1. Služby v IP síti	4-6
4.4.2. Kvalita služeb	4-7
4.4.3. Systém sledování služeb	4-8
4.5. Řešení dohledu IS	4-10
4.5.1. Nasazení elementárních systémů dohledu	4-10
4.5.2. Nasazení systémů pro dohled služeb a integraci informací	4-11
4.6. Způsoby provozování systémů pro dohled IS	4-12
4.6.1. Nasazení systémů pro dohled IS a zabezpečení lidských zdrojů	4-12
4.6.2. Nasazení systémů a zabezpečení lidských zdrojů externí organizací	4-12
4.6.3. Vyřešení dohledu a správy IS externí organizací (outsourcing)	4-13
5. Služby vyšších vrstev	5-1
5.1. Společné zásady budování vyšších služeb OSI modelu	5-1
5.2. Bezpečnost sítě ROWANet	5-1
5.2.1. Základní teze	5-2
5.2.2. Bezpečnostní prvky	5-3
5.3. Popis základních infrastrukturních služeb IP sítí	5-12
5.3.1. Návrh základní architektury služeb IP sítí	5-13
5.3.2. Služba DNS	5-13
5.3.3. Systém DHCP	5-17
5.3.4. Základní principy časové synchronizace – NTP	5-20
5.3.5. Adresářové služby	5-21
5.3.6. LDAP proxy jako integrační prvek adresářových služeb	5-26
5.4. Služby IP sítí nezbytné pro počáteční provoz infrastruktur	5-28
5.4.1. DNS	5-28
5.4.2. NTP	5-29
5.4.3. Firewall	5-29
5.5. Budování dalších služeb IP sítí	5-29
6. Aplikační vrstva	6-1
6.1. Informace	6-1
6.2. Zábava	6-1
6.3. Vzdělávání	6-2
6.4. Způsob realizace	6-2
6.4.1. Weby a portály	6-2
6.4.2. Vyhledávací služby	6-6
7. Správa systému, řízení a poskytování zdrojů	7-1
7.1. Serverhosting	7-2
7.2. Webhosting	7-2
7.3. Outsourcing	7-2
8. ROWANet z pohledu uživatele	8-1
8.1. Uživatelé ROWANetu	8-1
8.2. Propojovací síť	8-2
8.3. Zdroj informací	8-2
8.4. Data, Voice, Video	8-3
8.5. Bezpečnost sítě	8-3
8.6. Zdroj obživy	8-3
9. Navrhovaný postup prací	9-1
10. Přílohy	10-1

10.1. e-Europe	10-1
10.1.1. Quick win	10-3
10.1.2. Výběr cílů	10-3
10.1.3. Systém měření a vyhodnocování	10-4
10.1.4. Kriteria měření eEurope 2002	10-4
10.1.5. Kriteria měření služeb e-governmentu.....	10-6
10.1.6. Kriteria měření eEurope 2005	10-8
10.1.7. Současná pozice ČR.....	10-12
11. Literatura	11-1

Seznam obrázků:

Obrázek 3-1 VPN s využitím VLAN	3-5
Obrázek 3-2 Operace MPLS	3-7
Obrázek 3-3 MPLS značky	3-8
Obrázek 3-4 VPN s využitím MPLS	3-8
Obrázek 3-5 Operace se značkami ve VPN MPLS síti	3-9
Obrázek 3-6 VPN síť prostřednictvím MPLS	3-10
Obrázek 3-7 Směrování v MPLS síti poskytovatele služeb	3-11
Obrázek 3-8 Inter-VPN komunikace kontrolovaná firewallem	3-12
Obrázek 3-9 Příklad topologie Hub and Spoke na páteři WAN	3-16
Obrázek 3-10 Příklad topologie Ring na páteři WAN	3-17
Obrázek 3-11 Příklad topologie Multi ring na páteři WAN	3-18
Obrázek 3-12 Příklad topologie Hub and Spoke na distribuční vrstvě	3-19
Obrázek 3-13 Příklad topologie Ring na distribuční vrstvě WAN	3-19
Obrázek 3-14 Příklad topologie Multi ring na distribuční vrstvě WAN	3-20
Obrázek 3-15 Příklad částečné redundance cest	3-21
Obrázek 3-16 Redundance fyzických spojů	3-22
Obrázek 3-17 Hierarchické dělení adresního prostoru	3-32
Obrázek 3-18 Plný Internet	3-36
Obrázek 3-19 Centrálně filtrovaný Internet	3-37
Obrázek 3-20 MPLS VPN CsC - výměna směrovacích informací	3-39
Obrázek 4-1 Funkčnost komplexního fault managementu	4-6
Obrázek 5-1 Bezpečné připojení organizace k Internetu	5-3
Obrázek 5-2 Design sítí s ID systémy	5-6
Obrázek 5-3 Příklad AVO souborového systému	5-7
Obrázek 5-4 Příklad AVO HTTP a FTP komunikace	5-8
Obrázek 5-5 Příklad AVO SMTP komunikace	5-8
Obrázek 5-6 Příklad šifrované komunikace	5-12
Obrázek 5-7 Varianty směrování zpráv SMTP	5-16
Obrázek 5-8 Příklad hierarchie adresářového stromu	5-22
Obrázek 5-9 Synchronizace uživatelských účtů proti adresářové službě	5-22
Obrázek 5-10 Logický model spolupráce adresářových služeb na KU	5-25
Obrázek 5-11 Princip chování LDAP proxy	5-26

Seznam tabulek:

Tabulka 5-1 Porovnání Host versus Network based IDS	5-4
Tabulka 5-2 Soupis RFC, která se vztahují k použití LDAP	5-28

1. Zadání

Cílem projektu je vypracovat systémový projekt, který bude obsahovat následující části:

- návrh topologie (logika sítě na úrovni IP),
- variantní návrh služeb sítě,
- návrh agendy,
- návrh adresace, návrh IP plánu, DNS, AD,
- bezpečnostní služby (FW, AVO),
- správa systémů (management, personální zajištění, provozní zajištění),
- návrh propojení s externími sítěmi (KIVS, GOVBONE),
- hrubý odhad HW řešení,
- navržené řešení bude založeno na využití mezinárodních otevřených standardů na rozhraních mezi objednatelem a ostatními subjekty.

2. Všeobecný přehled

2.1. Účel

Primárním záměrem – centrální vizí je podpořit rozvoj kraje Vysočina v regionu České republiky ve smyslu obecné teze „kraj, kde se dobře žije a podniká“. Výklad či obsah teze i postup a prostředky jejího naplnění mohou být různorodé.

Výklad, obsah

Jako občan, podnikatel či organizace potřebují řešit základní životní situace a potřeby:

- Komunikovat
data, hlas, video, 1:1, 1:n
- Být občanem
informace, operace, platby, ...
- Žít a bydlet
bydlení – domy, byty
sítě (energie, voda, kanalizace, komunikace, odpady)
zdravotnictví
handicapovaní občané
doprava
styk s úřady (legislativa,...)
- Rekreatovat se
rekreační objekty (chaty a chalupy)
sítě (energie, voda, kanalizace, komunikace)
hotely a penziony
doprava
styk s úřady (legislativa,...)
- Pracovat
zaměstnanost / nezaměstnanost
trh práce
handicapovaní občané
styk s úřady (legislativa,...)
- Podnikat
zaměstnání
produkty
styk s úřady (legislativa,...)
- Obchodovat
prodat, koupit, dopravit, ...

- Cítit se bezpečně
policie, zdravotnictví, hasiči, IZS, ...
- Bavit se
kultura (knihovny), sport, zájmy, ...

Prostředky, postup

Jedním z vhodných prostředků je intenzivní využití a rozvoj prostředků ICT v každodenním životě pro širokou a pestrou skupinu uživatelů – organizace a občané. V tomto případě můžeme hovořit o technokratickém naplňování dané teze, které je nutné rozdělit do několika na sebe logicky navazujících oblastí:

- formulace vize angažovanosti ICT,
- prostředky a nástroje ICT,
- koncepce, definice, standardy, formáty,
- oblasti spolupráce,
- ekonomika.

2.2. Cíl systémového projektu

Cíl systémového projektu je navrhnout možné technické řešení a zabezpečení komunikační infrastruktury a návazných služeb jakožto základního stavebního kamene, neboť se jedná o nutné podmínky pro rozvoj návazných prostředků a služeb ICT. Projekt je rozdělen na následující části:

- návrh topologie (logika sítě na úrovni IP),
- variantní návrh služeb sítě,
- návrh agendy,
- návrh adresace, návrh IP plánu, DNS, AD,
- bezpečnostní služby (FW, AVO),
- správa systémů (management, personální zajištění, provozní zajištění),
- návrh propojení s externími sítěmi (KIVS, GOVBONE),
- hrubý odhad HW řešení.

Navržené řešení bude založeno na využití mezinárodních otevřených standardů na rozhraních mezi objednatelem a ostatními subjekty.

2.3. Vzájemné vazby v rozvoji informačních technologií

Samotná komunikační infrastruktura či samotná síť nepřináší rozvoj oblasti či regionu sama o sobě. Existuje celá řada vzájemně se ovlivňujících faktorů. V následujícím textu jsou analyzovány ty nejčastější či nejzávažnější vzájemné vazby.

2.3.1. Cena komunikační infrastruktury

Čím je cena pro koncového uživatele nižší, tím je větší poptávka. Při stejné užité hodnotě obsahu dostupného přes komunikační infrastrukturu je víc uživatelů, kterým se vyplatí koupit si komunikační službu.

Čím je cena vyšší, tím více se vyplatí investovat do infrastruktury a je větší šance na růst konkurence v oblasti telekomunikací.

Čím je cena nižší, tím více se vyplatí investovat do obsahu, protože je větší šance na návratnost (více zákazníků při stejných nákladech).

Čím je nižší cena připojení a čím je větší nabídka obsahu, tím více lidí bude přemýšlet o investici do svého vzdělání a tím více se jich rozhodne do svého vzdělání investovat (nejen peníze, ale i svoje úsilí a obětuje pohodlí).

Čím více bude uživatelů, tím se dříve navrátí investice do telekomunikační infrastruktury i investice do obsahu.

Čím více je uživatelů, tím je větší šance pro více poskytovatelů služeb, že budou mít zisk. Čím více je poskytovatelů služeb (obsahu zejména), tím vyšší hodnotu má obsah dostupný přes komunikační infrastrukturu a tím více lidí si koupí služby komunikační infrastruktury i služby poskytování obsahu.

2.3.2. Kritické množství a kritický čas

Existuje určité kritické množství a kritické tempo růstu, při kterém se nedaří a kde je téměř každá investice ztrátová. Teprve nad touto hranicí je šance na zisk. Dlouhodobé trvání stavu kritického množství vede k odumírání a ke kolapsu.

Mez kritického množství je dynamická a je ovlivňována globálními vlivy nezávislými na regionu nebo celé ČR. Takovými vlivy jsou světové ceny technologií, světové ceny know-how, světová konkurence. Všeobecně v oblasti ICT platí, že míra zisku se stárnutím technologie klesá. Míra zisku roste s velikostí trhu. Tedy malý trh má relativně větší kritické množství (měřeno k velikosti trhu v %) a dřívější okamžik propadu pod kritické množství než velký trh.

2.3.3. Dostupnost telekomunikační infrastruktury

Čím je daná oblast méně osídlena, tím vyšší relativní náklady má poskytovatel na zřízení a provoz telekomunikační služby.

Čím je v dané oblasti nižší příjmová úroveň, tím hůře vychází zákazníkům vnímaný poměr mezi cenou komunikační služby a hodnotou obsahu. Obsah většinou šetří čas a práci a obojí má v oblasti s nižší příjmovou úrovní menší cenu.

Čím vyšší je zájem zákazníků o telekomunikační služby, tím dříve se zaplatí investice do infrastruktury a je lepší šance na zisk poskytovatele. Proto budou poskytovatelé spíše investovat do oblastí s větší poptávkou. Proto bude dříve konkurence v oblastech kde je větší šance na zisk.

Čím je hustší osídlení, tím větší je konkurence alternativních řešení nevyužívajících ICT (vyplatí se třeba osobní návštěva, existují dostupné levnější a rychlejší dopravní služby). Čím řidší osídlení, tím jsou průměrné vzdálenosti větší a konkurence alternativních řešení je menší. Proto je větší šance na vítězství elektronické služby v oblastech s nižší hustotou osídlení z pohledu uživatele. Významnou roli ale hraje konzervatismus a vzdělání.

Vzdělání může být jedním z významných obsahů podporujících využívání telekomunikačních služeb v řídko osídlených oblastech.

2.3.4. Informační vzdělanost

Čím vyšší je vzdělanost v oblasti využití ICT (nezaměňovat se znalostí ICT), tím je více lidí, kteří mají představu k čemu ICT použít, a tedy kteří jsou schopni vyhodnotit věrohodně, zda se jim vyplatí nebo ne. Pokud tuto vzdělanost nemají, tak se budou rozhodovat podle něčeho jiného a ani pozitivní objektivní situace jejich rozhodnutí neovlivní. Tedy ani velmi nízké ceny, ani velmi vysoká kvalita obsahu jejich rozhodnutí pozitivně neovlivní. A v případě náhodného nákupu nebudou schopni (statisticky významně) získat přínos pro sebe a tedy nebudou hodnotit výsledek pozitivně. Tím negativně ovlivní postoj ostatních, kteří také nebudou mít potřebné schopnosti.

Čím vyšší bude kvalita obsahu a nižší cena telekomunikačních služeb, tím pozitivněji budou absolventi vzdělávání hodnotit jeho přínos a tím více ovlivní další lidi k motivaci se vzdělávat (investovat do svého vzdělání). Čím nižší bude kvalita obsahu a čím vyšší cena služeb, tedy čím menší bude počet uživatelů služeb, tím více absolventů vzdělávacích kurzů bude hodnotit poměr vynaloženého úsilí k osobnímu přínosu negativně. To zablokuje zájem dalších adeptů a oslabí důvěru k ICT celkově. Nedůvěra se bude velmi dlouho a velmi těžko odstraňovat.

Čím vyšší bude vzdělanost v užití ICT, tím větší bude počet lidí, kteří budou moci rozšířit nabídku obsahu a to jak v oblasti vzdělávání v jiných oborech, tak v nabídce jiných služeb. Tím bude i vyšší nabídka obsahu a tedy i přínos pro další adepty vzdělávání.

Je tu i jazykové specifikum obsahu. Není šance postavit rozvoj ICT v ČR na představě zajištění obsahu v jiném jazyce než v češtině. Představa, že velké množství lidí porovnatelné s kritickým množstvím pro rozvoj infrastruktury a dalšího obsahu se v průběhu přijatelné doby (tedy do 2 let) naučí cizí jazyk tak, aby obsah mohli využívat je nereálná. Investice ze strany uživatele je tak obrovská (i kdyby vše bylo zadarmo a uživatel musel investovat jen úsilí a pohodlí) a to obzvláště pro lidi středního a vyššího věku, že není šance dosáhnout (pro významné množství lidí) výhodného poměru mezi obsahem a náklady ze strany uživatele (a to ani tehdy, pokud by počítače a internet byly zadarmo). To znamená, že pouze obsah v češtině může být tahounem rozvoje ICT v ČR a tedy i v jednotlivých regionech.

2.3.5. Moderní veřejné služby

On-line veřejné služby (služby veřejné správy) jsou součástí obsahu. Uživatel je chápán jako plus při rozhodování o investici do vzdělání i o investici do komunikačních služeb. Čím častěji a čím více mu ušetří jiných nákladů, tím větší bude pro něj jejich hodnota.

Větší šanci na opakovatelnost použití on-line veřejných služeb i větší šanci na přínos elektronických služeb ICT mají firmy a to zejména malé a střední. Těch je také velké množství v porovnání s velkými firmami. Tyto firmy jsou také zajímavé vzhledem k počtu pro poskytovatele telekomunikačních služeb. Také úspora pracnosti ze strany VS je zajímavá vzhledem k počtu subjektů.

Malé a střední firmy jsou zdrojem rozvoje obsahu. Nemají však sílu na rychlý vývoj znalostí v této oblasti. Čím více malých firem bude mít znalosti a motivaci ve využití ICT, tím více jich bude používat služby e-governmentu a tím lepší a rozsáhlejší bude obsah nabízený koncovým uživatelům (zákazníkům firem). Čím více bude obsahu, tím více bude uživatelů a tím bude menší tlak ze strany uživatelů na snižování cen komunikačních služeb. Čím více bude uživatelů, tím větší bude objem peněz v oblasti telekomunikačního trhu a tím tvrdší bude konkurenční prostředí na telekomunikačním trhu. **Stimulace malých a středních firem k praktickému užití ICT vede k rozvoji obsahu. Má multiplikační efekt. Poskytování služeb e-governmentu pro tuto cílovou skupinu spolu s podporou vzdělání v užití ICT a podporou šíření know-how pro tyto firmy může mít velmi stimulující vliv na rozvoj ICT a vznik konkurenčního prostředí v telekomunikacích.**

Poskytování moderních veřejných služeb pouze on-line oslovuje jen malou část obyvatelstva. Nemá rychlý a pozitivní dopad na větší množství lidí. Je problematický z hlediska sociálních skupin. Oslovuje pravděpodobně zejména mladé a vzdělané občany ve vyšší příjmové kategorii. Nebude oslovovat vyšší věkové kategorie (vyšší vzdělanostní bariéra), ani velký počet občanů s podprůměrnou životní úrovní (platby za ICT jsou neúnosnou zátěží i při velmi nízkých cenách, lidé z těchto vrstev mají většinou jiné priority).

Implementace on-line služeb státu bývá většinou spojena i s využitím ICT ve vnitřních procesech (back-office). Využití ICT ve vnitřních procesech a techniky a procesy potřebné k zajištění on-line služeb je možné využít k poskytování moderních veřejných služeb i jinak než on-line. Tím je možné oslovit mnohem větší počet občanů a to i těch sociálních skupin, které on-line přístup neoslovuje. **Zejména efekt dostupnosti všech veřejných služeb v lokalitě vybrané občanem (např. v libovolném úřadě) může mít velmi pozitivní odezvu a je velmi snadno dosažitelný pokud bude zvládnuta problematika on-line moderních veřejných služeb.**

Veřejná správa je také zákazníkem ICT. S rostoucím uplatněním ICT v praktickém životě bude její vliv jako zákazníka klesat (v případě úspěchu). Počet uživatelů a objemy peněz investovaných do ICT občany a firmami porostou mnohem rychleji, než objem peněz investovaných VS (není podstatné zda formou nákupu technologií nebo formou nákupu služeb). Objem služeb VS se nebude zvyšovat takovým tempem, jako objem elektronických služeb poskytovaných komerčními subjekty. Chování veřejné správy jako zákazníka bude více ovlivňovat ICT v blízké budoucnosti než později, je tedy důležitější teď, než tomu bude v budoucnu. Chování veřejné správy může značně ovlivnit rozvoj ICT v blízké budoucnosti a může být značným stimulačním prvkem a nebo brzdou.

Objem využití ICT ve VS bude postupně růst. Stále více agend bude v elektronické podobě, stále více činností bude podporováno ICT. To bude vytvářet tlak na zvyšování nákladů na rozvoj a provoz ICT ve VS. Pokud bude rozvoj informační společnosti dostatečně rychlý a výrazný a bude rychle dosažen kritický objem, tak se začnou jednotkové ceny snižovat silící konkurencí.

Klesající ceny budou platné také pro VS. Proto jsou budoucí náklady VS na ICT závislé na rozvoji informační společnosti. Čím rychleji a více se rozvine, tím nižší budou náklady VS na ICT v budoucnu a tím vyšší bude efekt on-line veřejných služeb a nižší nároky na jiné náklady VS.

2.3.6. Životní úroveň

Čím vyšší bude průměrná životní úroveň, tím více lidí bude nakupovat telekomunikační služby, protože pro ně nebude tak významný výdaj. Tím bude menší tlak na snižování ceny telekomunikačních služeb ze strany uživatelů a tím nižší bude kritické množství. Čím nižší bude kritické množství, tím větší šanci bude mít konkurence na telekomunikačním trhu. Čím vyšší bude konkurence a větší potenciál trhu (šance získat zákazníka), tím budou nižší ceny a tedy více zákazníků.

Naopak, čím nižší bude životní úroveň, tím hůře vznikne konkurence a tím hůře půjde snižovat ceny.

Čím rozvinutější bude informační společnost v regionu, tím lepší budou podmínky pro investice a lepší konkurenceschopnost pracovní síly. Čím vyšší investice a čím méně nezaměstnaných, tím vyšší životní úroveň.

2.3.7. Prostředí pro elektronické podnikání

Čím lepší prostředí pro elektronické podnikání, tím lepší nabídka obsahu. Čím lepší nabídka obsahu, tím více potencionálních zákazníků. Čím více zákazníků, tím více investic do elektronického podnikání. Čím lepší prostředí pro elektronické podnikání, tím nižší ceny telekomunikačních služeb (dvojitý efekt – přímý vliv lepšího prostředí + větší počet uživatelů).

Čím větší nabídka obsahu a čím nižší ceny telekomunikačních služeb, tím menší kritické množství a tím větší úspěšnost elektronického podnikání. Čím větší úspěšnost tím méně nezaměstnaných a tím vyšší životní úroveň.

Objem telekomunikačního trhu může znatelně zvýšit pouze komerční využití. VS nemůže zvýšit objem vynakládaných prostředků na mnohonásobky.

2.3.8. Růst objemu a demonopolizace telekomunikačního trhu

Pouze rychlé násobné zvětšení objemu telekomunikačního trhu (celkové množství peněz utracených za telekomunikační služby) může zavést fungující konkurenci. Pomalé nebo žádné zvětšení objemu telekomunikačního trhu nemůže nic vyřešit (jen za cenu obřích ztrát dominantního operátora). Hrubé kalkulace ukazují, že k hladkému zavedení konkurenčního prostředí během 2 let je třeba zvětšit trh asi 3krát. K zavedení konkurenčního trhu za 5 let je nutné zvětšení trhu přibližně 5krát. To není objem poskytovaných služeb, ale množství peněz. Při žádaném poklesu ceny bude takový růst doprovázen příslušně vyšším růstem objemu služeb. Přitom telekomunikační trh v ČR není tak zaostalý, aby měl prakticky neomezené možnosti růstu.

Čím později tento proces proběhne a čím pomaleji bude probíhat, tím je menší šance na úspěch a velmi rychle se bude snižovat šance na realizaci vůbec. Např. v případě, že má současný telekomunikační trh 10 % služeb budoucího konkurenčního rozvinutého trhu a zavedení konkurence proběhne v období 5 let s okamžitým startem a po zavedení konkurence budou jednotkové ceny poloviční oproti současným, tak je to právě limitní případ. Tj. v okamžiku dosažení minimální hranice konkurenčního chování na telekomunikačním trhu bude trh nasycen. V případě stejných výchozích podmínek však bude ke vzniku konkurenčního prostředí stačit jen dvouleté období, a trh bude po ukončení demonopolizace nasycen na méně než 50 % a investoři budou mít o co soutěžit a tedy za 5 let dosáhnou nižších jednotkových cen a zároveň mohou více investovat do rozvoje trhu a tedy i zvýšit nabídku i objem trhu.

Odložení startu 5letého období o jeden rok už znemožní úspěch zcela. Za 1 rok dojde k růstu výchozí pozice tak, že nebude možné dosáhnout konkurence před okamžikem nasycení trhu. Odložení startu rychlého 2letého období o jeden rok neznemožní dosažení cíle, ale situaci zhorší tím, že bude vyčerpáno více objemu trhu v regulovaných podmínkách a na opravdovou soutěž už nezbude tolik prostoru a tedy i výsledný efekt bude horší.

Existuje mezní rychlost zavádění konkurenčního trhu, pod kterou není možné dosáhnout úspěchu. Tato rychlost se s odkládáním začátku zvyšuje.

Čím později bude dosaženo konkurenčního prostředí, tím více objemu trhu bude vyčerpáno v regulovaném období a tím menší prostor bude mít konkurenční trh. Tím se také zhorší kvalita trhu i úroveň nabídky služeb.

2.3.9. Bezpečnost elektronických služeb

Samotná bezpečnost komunikačních služeb nic neřeší. Podstatná je opodstatněná důvěra uživatelů v bezpečnost obsahu. Pokud uživatelé nebudou mít důvěru v bezpečnost, tak nebudou služby používat.

Bezpečnost není sama od sebe. Chování uživatelů je podstatnou částí bezpečnosti. Pokud uživatelé budou správně informováni a budou mít přiměřené znalosti, budou moci sami pro sebe zajistit vyšší bezpečnost a nebudou podléhat panikám a nepodloženým fámám.

Samotné technologie bezpečnost nevyřeší. Pouze přiměřená technologie v rukou znalého uživatele má význam.

Podstatná je přiměřená vyvážená bezpečnost přizpůsobená potřebám a konkrétním podmínkám. Příliš vysoká úroveň bezpečnosti zvyšuje neoprávněně náklady a zhoršuje uživatelské vlastnosti nadměrnými bezpečnostními opatřeními, příliš nízká bezpečnost neopodstatněně zvyšuje rizika ztrát.

Pravděpodobně nejškodlivější je nevyvážená bezpečnost, tedy kombinace dílčí nadměrné bezpečnosti a nedostatečné bezpečnosti v ostatních oblastech. Ta kombinuje zvýšené náklady a zhoršené uživatelské vlastnosti se zvýšeným rizikem ztrát.

Nezanedbatelnou roli v bezpečnosti mají veřejné služby (služby státu v oblasti bezpečnosti).

Kromě specializovaných týmů zaměřených na potírání elektronické kriminality (což je kompetence státních orgánů) je to celá škála osvětových a podpůrných akcí včetně podpory výměny zkušeností a pomoci v hledání bezpečných řešení a omezování činností, které jsou zjevně v rozporu s dobrými mravy, a které poškozují občany.

Významnou úlohu hrají také dobré zkušenosti a standardy bezpečnostních technologií orientované zejména na zjednodušení užití z pohledu uživatele.

Rozvoj obsahu dává větší šance k jeho zneužití. Tedy čím více obsahu, tím vyšší bezpečnostní rizika.

To samé platí s rozšiřujícím se počtem uživatelů. Čím více uživatelů, tím větší nebezpečí zneužití a tím větší šance na publicitu.

Čím více bezpečnostních technik a rozdílů v bezpečnostních řešeních ve větším počtu služeb, tím komplikovanější užití pro uživatele, a tím větší efekt má standardizace v oblasti bezpečnosti.

Zbytečně drahá a komplikovaná bezpečnostní opatření omezují pohodlí uživatele a zhoršují poměr přínosů obsahu k nákladům (včetně potřebného úsilí uživatele). Čím je bezpečnostní opatření uživatelsky náročnější, tím méně je uživatelů.

Ignorování bezpečnosti, zejména ignorování hrozeb internetu, povede ke ztrátám uživatelů a ke ztrátě důvěry uživatelů i komerční sféry v efektivitu ICT. Nedostupnost bezpečnostních služeb, jejich nedostatečná kvalita nebo neúnosná cena bude mít podobné důsledky.

2.3.10. Negativní vazby

Tato kapitola stručně shrnuje podstatné negativní vazby. Každá může zablokovat či podstatně zhoršit situaci ve všech ostatních oblastech a tak být příčinou celkového neúspěchu:

- Vysoké ceny připojení - snižují počet uživatelů.
- Nedostatek znalostí a dovedností - snižuje počet uživatelů.
- Nedostatek obsahu nebo nízká kvalita či nesrozumitelnost obsahu - snižuje počet uživatelů.
- Špatné, nedostupné a problematické veřejné služby - stěžují postavení firem. To zhoršuje investice do obsahu a snižuje kupní sílu i zájem potencionálních uživatelů.
- Nízký počet uživatelů - zdrazuje služby, snižuje šance na zisk firem a zhoršuje nabídku a tím i poptávku.
- Nepřiměřeně náročná bezpečnostní opatření - snižuje počet uživatelů.
- Nedostatečná bezpečnostní opatření - snižují počet uživatelů.

3. Komunikační infrastruktura - síťové prostředí

3.1. Technologie WAN sítě

Existuje základní požadavek na transport či propojení více privátních sítí na bázi protokolu TCP/IP jednotlivých subjektů v rámci kraje Vysočina, případně sdílení společných zdrojů. V následujícím textu uvádíme teoretický úvod do technologií pro budování privátních sítí nad sdílenou infrastrukturou a rozvalu použitelnosti zmíněných technologií pro uvažovanou síť ROWANet.

3.1.1. Virtuální privátní síť

Síť provozovaná na jediné společné infrastruktuře, ale přitom vzájemně datově oddělené budeme nazývat **virtuální privátní síť – VPN** (*Virtual Private Networks*).

Společnou infrastrukturu budeme označovat jako **síť poskytovatele služeb** (*Service Provider Network*). Poskytovatelem služeb může být organizace poskytující pouze danou infrastrukturu jiným organizacím nebo organizace, která tuto infrastrukturu, kromě samotného poskytování jiným organizacím, využívá i pro vlastní účely.

Datový provoz mezi různými VPN sítěmi provozovanými několika organizacemi na jediné společné komunikační infrastruktuře poskytovatele služeb musí být za normálních okolností navzájem striktně oddělen. Případná vzájemná komunikace oddělených sítí musí probíhat pouze na základě přesných explicitně stanovených pravidel, odsouhlasených všemi stranami např. prostřednictvím specializovaného zařízení typu **firewall**.

Protože kapacita sdílené přenosové infrastruktury je vždy omezená a má být poskytována i jiným organizacím, je potřeba, aby měl poskytovatel sdílené sítě možnost definovat pro každou virtuální privátní síť kvalitu služby QoS (*Quality of Service*). Jedná se vždy o soubor několika parametrů určujících např. garantovanou kapacitu poskytnutého přenosového pásma, prioritu přenášených dat apod. Tyto parametry jsou součástí dohody mezi poskytovatelem sítě a zákazníkem – SLA (*Service Level Agreement*).

Virtuální privátní síť lze rozdělit na:

- Access VPN,
- Intranet a extranet VPN.

Pro implementaci těchto typů VPN se používají rozdílné technologie.

3.1.1.1. Access VPN

Tento druh VPN sítí poskytuje dočasný bezpečný vzdálený přístup mobilních uživatelů – jednotlivců nebo např. doma pracujících zaměstnanců (telecommuters) do podnikové sítě (extranet nebo intranet) přes veřejnou síť (síť poskytovatele služeb).

Tento typ VPN není předmětem tohoto materiálu.

3.1.1.2. Intranet a extranet VPN

Na rozdíl od předchozího typu je hlavním účelem těchto VPN sítí propojení vzdálených pracovišť v rámci jedné organizace (intranet) nebo zajištění řízeného datového přístupu mezi různými organizacemi (extranet) opět přes sdílenou veřejnou síť poskytovatele služeb.

Následují technologické možnosti budování tohoto typu VPN:

- IP tunel – GRE (Generic Routing Encapsulation), IPSec,
- virtuální okruh – (Frame Relay, ATM),
- Virtual LAN – over Gigabit Ethernet
- MPLS (Multiprotocol Label Switching) – IP nebo IP+ATM.

3.1.2. Volba technologie pro implementaci VPN v síti ROWANet

V předchozí kapitole jsme uvedli technologické možnosti pro implementaci VPN v rozlehle síti ROWANet .

Před volbou odpovídající technologie pro síť ROWANet shrneme nejdůležitější vlastnosti moderní robustní implementace VPN sítí.

Požadované vlastnosti:

- **konektivita „každý s každým“**,
- **rozšiřitelnost** – možnost snadným způsobem rozšiřovat síť, vytvářet nové VPN,
- **bezpečnost** – VPN musí poskytnout srovnatelnou úroveň bezpečnosti, jaká se dosahuje v klasických privátních sítích,
- **priorita** – VPN by měla mít prostředky pro odpovídající zpracování různých typů datových toků (časově citlivá data, přednostní data ...),
- **spolehlivost** – celá implementace by měla zaručovat vysokou dostupnost VPN sítí,
- **spravitelnost** - nezbytný je vhodný management VPN sítí, který umožní sledovat a případně účtovat poskytované služby.

3.1.2.1. IPsec-VPN

Jednou ze základních možností jak vybudovat virtuální privátní síť ve „veřejné“ síti s komunikačním prostředím TCP/IP (obecně v jakékoli veřejné síti poskytovatele služeb) jsou tzv. **IP tunely**, kdy je propojení jednotlivých oddělených částí privátní sítě přes sdílenou IP síť realizováno enkapsulací (zabalením) protokolu privátní sítě do protokolu sítě veřejné (IP v IP). Pro dosažení většího zabezpečení je možno tuto technologii kombinovat např. se standardizovanou technologií **IPSec**, která umožňuje data privátní sítě přenášena prostřednictvím sdílené IP sítě šifrovat.

Tato technologie VPN má nevýhody především v **omezené rozšiřitelnosti**, **zvýšené režii** na komunikačních prvcích i komunikačních spojkách (záhlaví enkapsulovaného protokolu) a také ve **vysokých nárocích na správu a řízení** sdílené IP sítě (konfigurace IP tunelů, nezávislost adresních schémat, směrovacích strategií, bezpečnostních pravidel apod.).

Vzhledem k rozsahu navrhované WAN sítě ROWANet a vzhledem k možnému rozsahu a množství privátních sítí propojujících jednotlivé subjekty veřejné samosprávy, ale i další organizace (např. HZS), nedoporučujeme tuto technologii z výše uvedených důvodů použít pro vytváření virtuálních privátních sítí nad infrastrukturou navrhované sítě ROWANet.

3.1.2.2. Frame Relay, ATM

Druhou možností implementace virtuálních privátních sítí je využití některé z technologií podporující vytváření virtuálních okruhů a cest. Za perspektivní technologie lze v tomto případě označit technologie Frame Relay nebo ATM implementované v síti poskytovatele služeb (v našem případě navrhovaná WAN síť ROWANet). Obě tyto technologie disponují prostředky pro vytváření **virtuálních transportních sítí**, tedy sítí **vzájemně oddělených na úrovni linkové vrstvy** modelu ISO/OSI, poskytujících určitou předem definovanou kvalitu služeb. Vlastní VPN jsou pak v síti poskytovatele služeb vytvářeny např. pomocí permanentních virtuálních okruhů (*PVC – Permanent Virtual Circuit*) propojujících jednotlivé části dané VPN. Toto řešení by tedy de-facto vedlo k vybudování privátní Frame Relay/ATM sítě ROWANet.

Pro realizaci komunikačních spojů transportní Frame Relay/ATM sítě lze použít digitální okruhy nebo využít infrastrukturu ATM sítě jiného poskytovatele.

Nevýhodou tohoto řešení VPN je především **vyšší cena komunikačních prvků** nutných pro vybudování sítě založené na této technologii.

Za další nevýhodu tohoto řešení lze označit i **vysoké nároky na správu a řízení transportní Frame Relay/ATM sítě** (např. konfigurace virtuálních spojů Frame Relay nebo ATM). Poměrná složitost spojově orientované (*connection-oriented*) technologie ATM rovněž klade zvýšené nároky na odbornost obsluhujícího personálu apod.

Velkou **výhodou** této technologie je to, že umožňuje budovat virtuální privátní sítě navzájem oddělené na úrovni druhé vrstvy modelu ISO/OSI, což zaručuje poměrně **vysoký stupeň bezpečnosti** takto vybudovaných virtuálních sítí.

3.1.2.3. VLAN over Gigabit Ethernet

Třetí možností implementace virtuálních privátních sítí nad infrastrukturou navrhované sítě ROWANet je využití technologie Virtuálních LAN sítí nad přepínanou infrastrukturou.

Přes celou páteř se mohou rozprostírat prostřednictvím VLAN jednotlivé VPN. V centrální lokalitě KÚ Vysočina se bude nacházet L3 switch, který zajistí směrování a filtraci provozu mezi jednotlivými VPN, případně provozu do externích sítí a Internetu.

Princip fungování

Síťová zařízení mohou do každého rámce přidávat značku, která říká, do které virtuální sítě daný rámec patří. Takové rámce jsou pak doručeny pouze těm zařízením, která patří do dané virtuální LAN sítě. Značkovat rámce pak mohou buď koncové stanice nebo mezilehlé síťové prvky (přepínače).

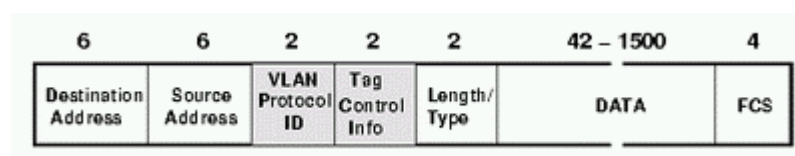
Nejčastějším kritériem je přidělování značek podle portu přepínače, na kterém je koncová síť nebo stanice umístěna. Tak dosáhneme oddělení jednotlivých počítačů (nebo celých sítí) do samostatných virtuálních sítí.

Detaily

Pro "virtuální přepínané síť" ve zkratce VLAN je dnes standardem protokol 802.1Q. Standard 802.1Q přidá do každého rámce 4 bajty identifikace tzv. virtuální sítě. Takový rámec se pak měl dostat do koncové stanice připravené na VLAN, která si pak sama rozhodne, jak s takovým rámcem naloží. Každý rámec měl být zbaven této nově přidané hlavičky a předán vyšší vrstvě. Ta díky tomuto řešení nemusela být měněna. Pro stanice, které na VLAN nejsou připravené a zvládají tedy pouze jedinou LAN síť odstraňuje tuto značku přepínač, ke kterému je stanice připojena.

Nový formát rámce

Jak už bylo řečeno, do ethernetového rámce (a nejen do něj, ale i do jiných technologií, např. Token Ring), přibyl 4 bajty a rámec tedy vypadá následovně:



v případě ethernetu se tedy jedná o Type Encoded rámec, do kterého se přidávají značky za cílovou a zdrojovou adresu (v sítích Token Ring a FDDI se tyto značky zapouzdřují až za SNAP). Pole Tag Control Info je šestnáctibitové a dělí se na tři části (priority - 3 bity, CFI - 1 bit, VLAN ID - 12 bitů). Význam jednotlivých polí je následující:

VLAN Protocol ID je šestnáctibitový identifikátor typu rámce a obsahuje hodnotu 0x8100. Pro VLAN zařízení je to identifikace toho, že následující dva bajty obsahují informace o VLAN

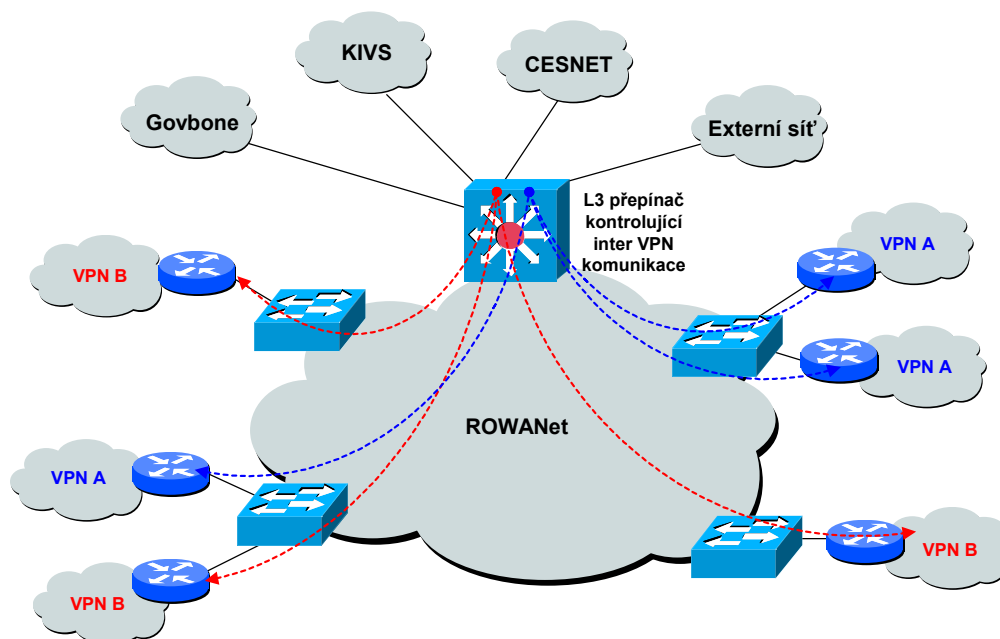
Priority obsahuje tříbitovou hodnotu uživatelské priority rámce. Ethernet sám o sobě neobsahuje žádné řízení priority rámců. Původně měl pro takové řízení vzniknout standard 802.1p, který byl ovšem nakonec zahrnut standardu 802.1Q. Priorita rámce je informace pro přepínače o tom, do které fronty Class of Service si má rámec zařadit.

Canonical Format Indicator (CFI) definuje v jakém pořadí jsou přenášeny bity v rámci (vztahuje se až na vnitřní část rámce). Kanonickým tvarem je little endian (ten je používán v ethernetu), nekanonickým je big endian (používaný v Token Ringu a FDDI). Smysl tohoto příznaku je přehozený, protože 0 znamená kanonický tvar (tento bit se původně jmenovat TREN - Token Ring ENcapsulation a byl z politických důvodů přejmenován).

VLAN Identifier je dvanáctibitové číslo pro zaznamenání čísla VLAN. To nám dává celkový počet 4096 maximálně možných VLAN. Dvě čísla jsou rezervovaná a to 0xFFF pro budoucí použití a 0 znamená, že rámec není označen jako VLAN, ale používá se pouze pro identifikaci priority rámce.

VPN v síti ROWANet prostřednictvím VLAN

Následující obrázek schématicky znázorňuje budování VPN sítě s využitím technologie VLAN.



Obrázek 3-1 VPN s využitím VLAN

Jednotlivé VPN se rozprostírají prostřednictvím VLAN do jednotlivých lokalit. Komunikaci mezi jednotlivými VPN zajišťuje výkonný centrální L3 přepínač. Na něm se prostřednictvím access listů též uplatňuje bezpečnostní politika.

Jednotlivé organizace budou mít přivedeny do své lokality příslušné VPN (VLAN). Ty budou vyvedeny na vybraném portu přepínače v dané lokalitě a měly by být zakončeny na směrovači nebo firewallu jednotlivých organizací.

Externí sítě mohou být připojeny buď prostřednictvím firewallu k centrálnímu L3 přepínači nebo v méně bezpečné ale ekonomičtější variantě přímo k centrálnímu L3 přepínači, který bude zajišťovat filtraci provozu.

Pokud bude zvolena varianta bez firewallu, bylo by vhodné vybavit L3 přepínač firewall modulem.

Na žádost KÚ Vysočina doplňujeme pro tuto variantu vhodný hardware. Návrh hardware byl konzultován s firmou AutoCont jakožto tvůrcem technického projektu CWDM sítě.

Do centrálních lokalit (KÚ Vysočina a Optokon) doporučujeme nasazení L3 přepínačů řady 6500.

Do ostatních lokalit doporučujeme nasazení L3 přepínačů Cisco Catalyst 3750 Metro, které umožňují softwarový upgrade na MPLS PE směrovač.

3.1.2.4. Multiprotocol Label Switching

Čtvrtou možností budování virtuálních privátních sítí nad infrastrukturou navrhované IP sítě ROWANet, která řeší nevýhody výše zmíněných technologií, je technologie MPLS (*Multiprotocol Label Switching*).

Vzhledem k tomu, že považujeme tuto technologii za obecně **nejvhodnější technologii** pro budování VPN sítí, uvedeme v následujících několika kapitolách tohoto dokumentu nejen její podrobnější popis, ale rovněž i základní principy vlastní implementace této technologie v prostředí navrhované IP sítě ROWANet.

Technologie MPLS (*Multiprotocol Label Switching*) je vytvořena na základě technologie Tag Switching vyvinuté firmou Cisco Systems.

Standardizace technologie MPLS probíhá prostřednictvím organizace IETF (*Internet Engineering Task Force*).

Technologie MPLS je založena na principu označování paketů 3. vrstvy OSI modelu speciálními značkami (*label*). Pakety jsou pak v síti dopraveny na základě těchto značek a odpadá tak časově a procesorově náročné prohledávání směrovacích tabulek.

Značky – *labels* určují cestu paketů a např. typ služby (*Class of Service*).

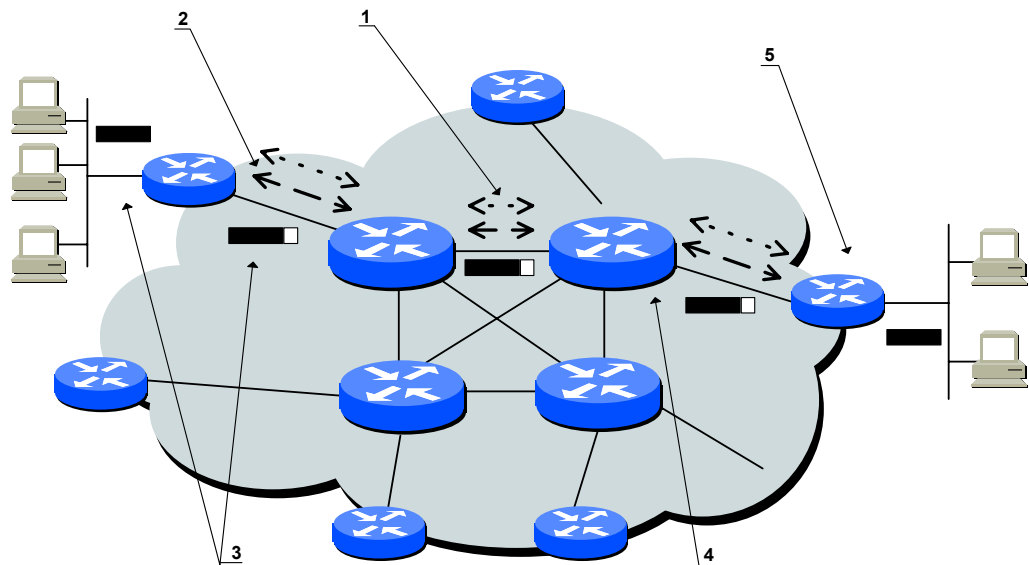
Ve vstupním bodě do MPLS sítě jsou přicházející pakety zpracovány a každému je přiřazena odpovídající značka. V jádru MPLS sítě komunikační prvky směrují (přepínají) pakety na základě předřazené značky. Všechny procesorově náročné analýzy, filtrace a vyhodnocení se realizují pouze jednou ve vstupním bodě. Ve výstupním bodě MPLS sítě je značka s paketů odstraněna a pakety jsou odeslány do cílové sítě.

MPLS terminologie:

- **Edge Label Switch Router** (*Edge LSR*) – zařízení na okraji MPLS sítě realizující počáteční zpracování a klasifikaci příchozích paketů, aplikaci první značky na cestě paketu. Tímto komunikačním prvkem může být buď směrovač, nebo ATM přepínač se zabudovanými směrovacími funkcemi.
- **Label Switch Router** (*LSR*) – zařízení umístěné v jádru MPLS sítě, které přepíná označované pakety podle předem ustavených přepínacích tabulek. Tímto komunikačním prvkem může být opět buď směrovač, nebo ATM přepínač se zabudovanými směrovacími funkcemi.
- **Label Distribution Protocol** (*LDP*) – protokol, který zajišťuje komunikaci mezi komunikačními prvky na okraji i v jádru MPLS sítě. Ve spolupráci s některým z IGP (Interior Gateway Protocol) – např. OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Protocol), IS-IS (Intermediate System to Intermediate System).
- **Label Switched Path** (*LSP*) – cesta MPLS sítě definovaná posloupností všech značek přiřazených mezi dvěma koncovými body MPLS sítě. LSP může být definována buď dynamicky nebo staticky.

- **Label** – značka; jedná se o záhlaví paketu, které je používáno zařízením typu LSR pro forwarding paketů. Formát záhlaví závisí na typu sítě, ve které je technologie MPLS implementována. V prostředí sítě postavených primárně na komunikačních prvcích typu směrovač je značka oddělené 32bitové záhlaví. V sítích typu ATM je značka umisťována do identifikátoru VCI/VPI (*Virtual Path Identifier/Virtual Channel Identifier*) v záhlaví ATM buňky. V jádru sítě pak zařízení typu LSR čtou pouze značku a ne celé záhlaví paketu. Velký význam pro rozšiřitelnost řešení založeného na MPLS má fakt, že značky – labels mají pouze lokální význam mezi dvěma komunikujícími zařízeními.

Následující obrázek a doprovodný text ukazují základní operace MPLS.

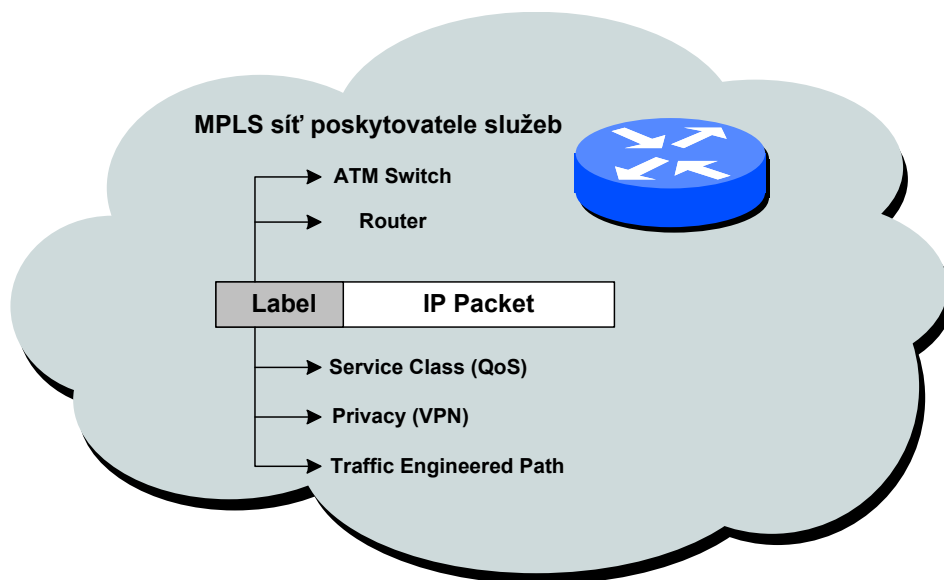


Obrázek 3-2 Operace MPLS

Směrovače nebo IP+ATM přepínače si v MPLS síti poskytovatele služeb vyměňují směrovací informace prostřednictvím IGP protokolu (OSPF, IS-IS, EIGRP).

1. LDP protokol využívá směrovací topologii obsaženou ve směrovacích tabulkách pro dohodu (výměnu) značek mezi přímo sousedícími zařízeními. Tato část operace vytvoří LSP cesty mezi koncovými body MPLS sítě. Značky jsou přidělovány automaticky bez nutnosti manuální konfigurace.
2. Paket vstupuje do MPLS sítě prostřednictvím zařízení typu Edge LSR, kde je zpracován a může zde být např. určeno jaký typ služby daný paket požaduje (QoS, využití přenosového pásma). Na základě směrovacích požadavků a požadavků na typ služby vybere a předřadí zařízení Edge LSR příslušnou značku k paketu a paket je vyslán dál do sítě MPLS.
3. Zařízení LSR v jádru sítě přečte značku na každém paketu a nahradí ji novou značku na základě přepínací tabulky (vybudované pomocí LDP) a pošle paket dál. Tato operace se opakuje ve všech LSR zařízeních v jádru sítě.
4. Výstupní zařízení Edge LSR odstraní z paketu značku, přečte hlavičku paketu a vyšle paket do cílové sítě.

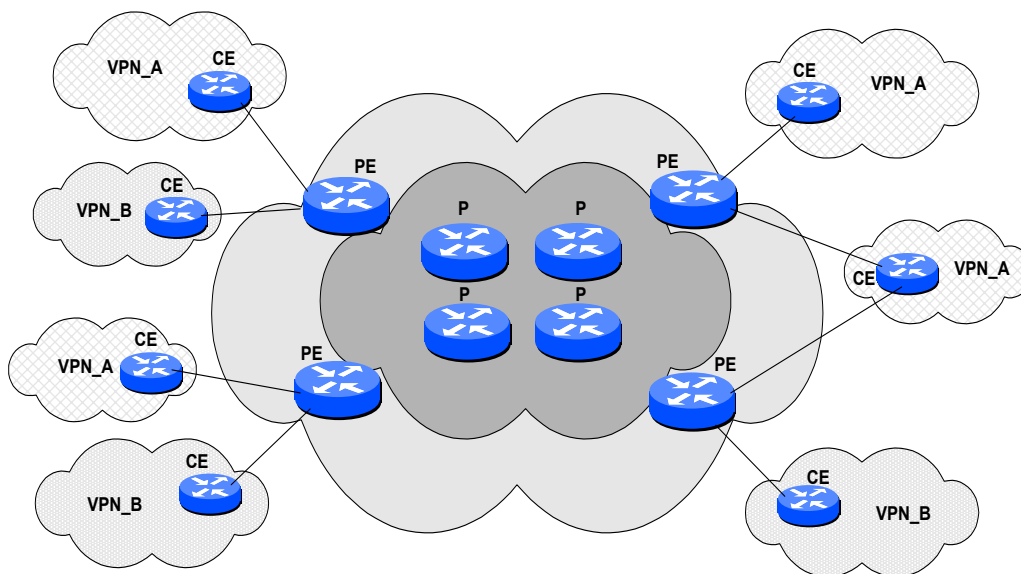
Značky v MPLS síti slouží nejen pro určení cesty paketu, ale je možné vytvářet s jejich pomocí VPN sítě, definovat QoS (*Quality of Service*), případně explicitně určovat kudy má procházet určitý datový tok (*traffic engineering*). Protože značky mají pouze lokální význam mezi dvěma sousedícími zařízeními, je prakticky nemožné vyčerpat všechny možné značky při budování rozlehlých sítí.



Obrázek 3-3 MPLS značky

VPN prostřednictvím MPLS

Následující obrázek schématicky znázorňuje budování VPN sítí s využitím technologie MPLS.



Obrázek 3-4 VPN s využitím MPLS

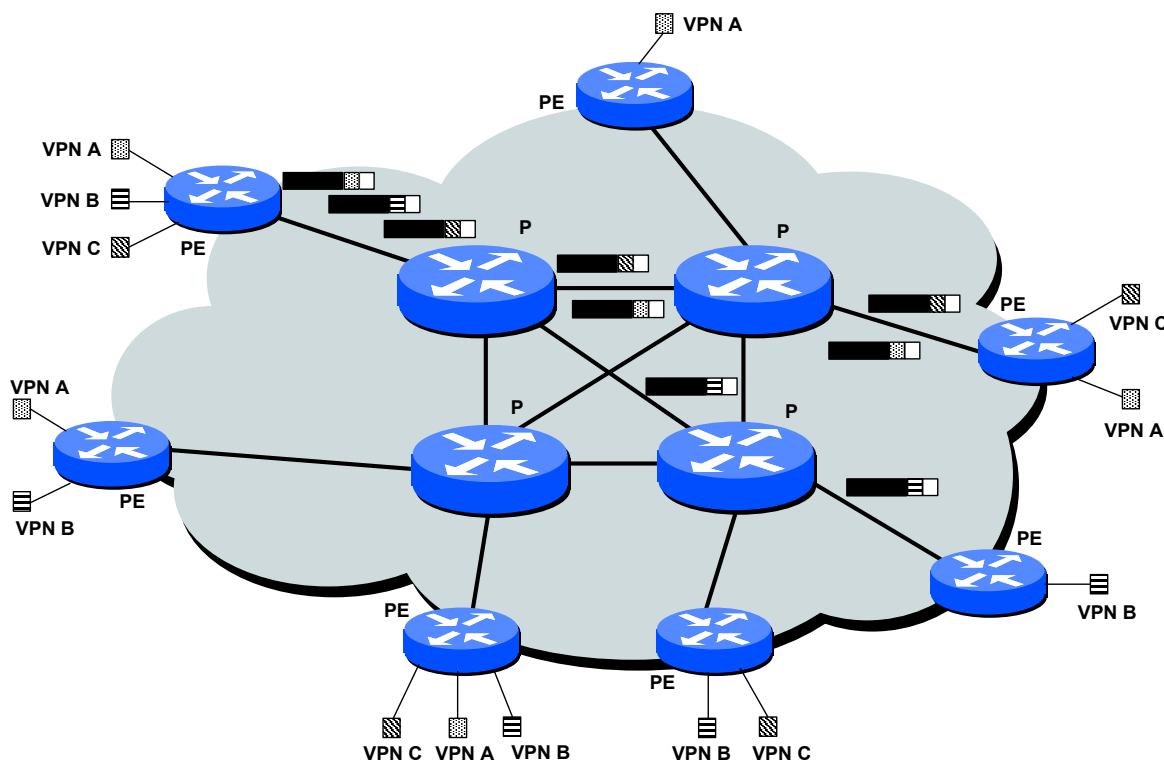
Použité zkratky:

- **P** – *provider router* – směrovač v síti poskytovatele služeb, v terminologii MPLS jde o **LSR** (*Label Switch Router*).
- **PE** – *provider edge router* – směrovač na okraji MPLS sítě, v terminologii MPLS jde o **Edge LSR** (*Edge Label Switch Router*).
- **CE** – *customer edge router* – směrovač na okraji zákaznické síti, připojující tuto síť k síti poskytovatele (k PE směrovači).

PE směrovače na okraji MPLS sítě provádějí operace přiřazení značky (značek) k paketu přicházejícímu ze zákaznické sítě a odstranění značky z paketů přicházejících z MPLS sítě.

Princip budování VPN v síti MPLS spočívá v možnosti opatřit každý paket vstupující do MPLS sítě ze sítě zákazníka VPN značkou tzv. RD (*Route Distinguisher*), jednoznačně identifikující tuto virtuální privátní síť. Tato operace proběhne na okraji MPLS sítě v PE směrovači (*Edge LSR*) na základě vstupního portu (může se jednat i o virtuální port) směrovače, kterým přijde daný paket. Tento směrovač dále, v souladu s principy fungování MPLS sítě, předradí před paket označený VPN značkou další značku označující "next hop" v MPLS síti a vyšle takto upravený paket dále do MPLS sítě poskytovatele služeb.

Následující obrázek zachycuje zmíněnou operaci.

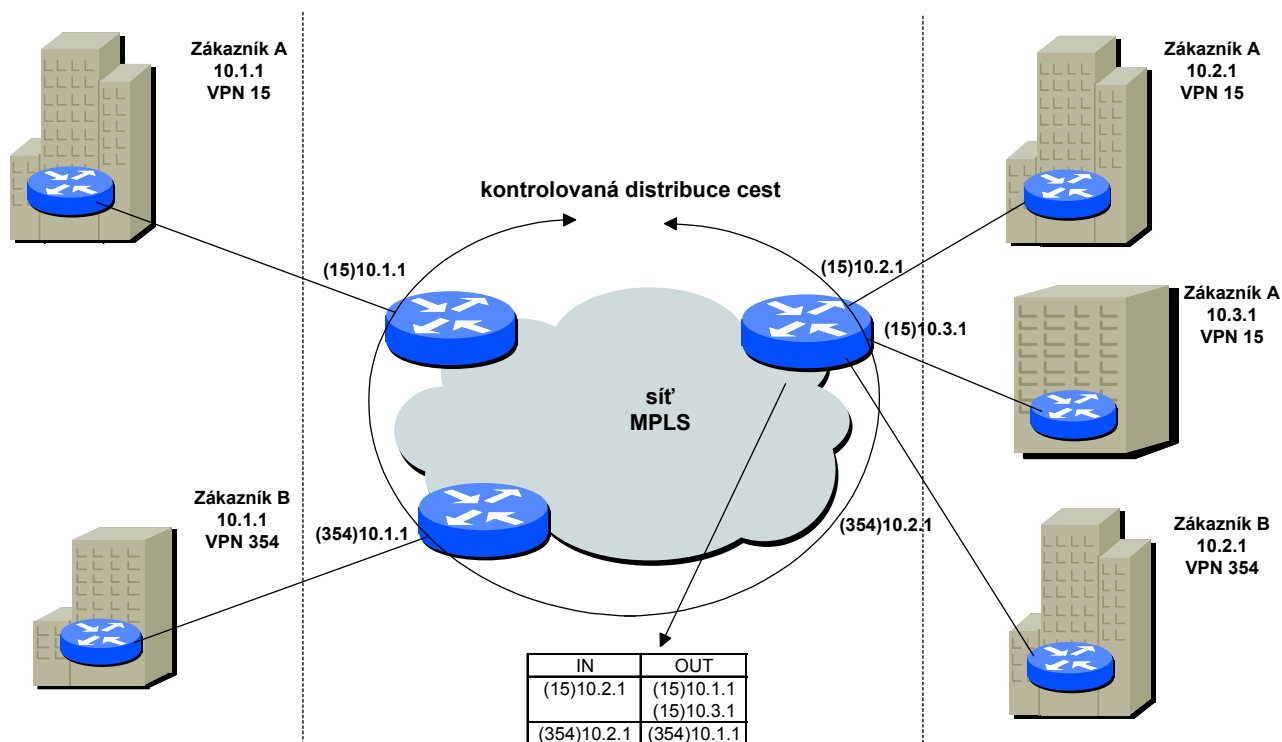


Obrázek 3-5 Operace se značkami ve VPN MPLS síti

Tím, že jsou cílové adresy IP paketů z jednotlivých VPN doplněny o VPN značku, je zajištěna jedinečnost těchto adres v rámci celé sítě poskytovatele služeb.

MPLS adresní prostory jednotlivých VPN sítí jsou pak vždy navzájem disjunktní, a to i v případě, když se z hlediska IP překrývají.

Je tedy možné využít síť poskytovatele služeb pro propojování lokalit zákaznických sítí, jejichž IP adresní prostor je v konfliktu s IP adresním prostorem jiných, již připojených VPN sítí.



Obrázek 3-6 VPN síť prostřednictvím MPLS

Směrování v MPLS síti poskytovatele služeb

Problematicku směrování v MPLS síti poskytovatele služeb lze rozdělit takto:

- směrování v páteřní síti,
- výměna směrovacích informací mezi lokalitou zákaznické sítě a okrajem páteřní sítě (rozhraní CE – PE),
- výměna směrovacích informací mezi lokalitami zákaznických sítí.

Směrování v páteřní síti

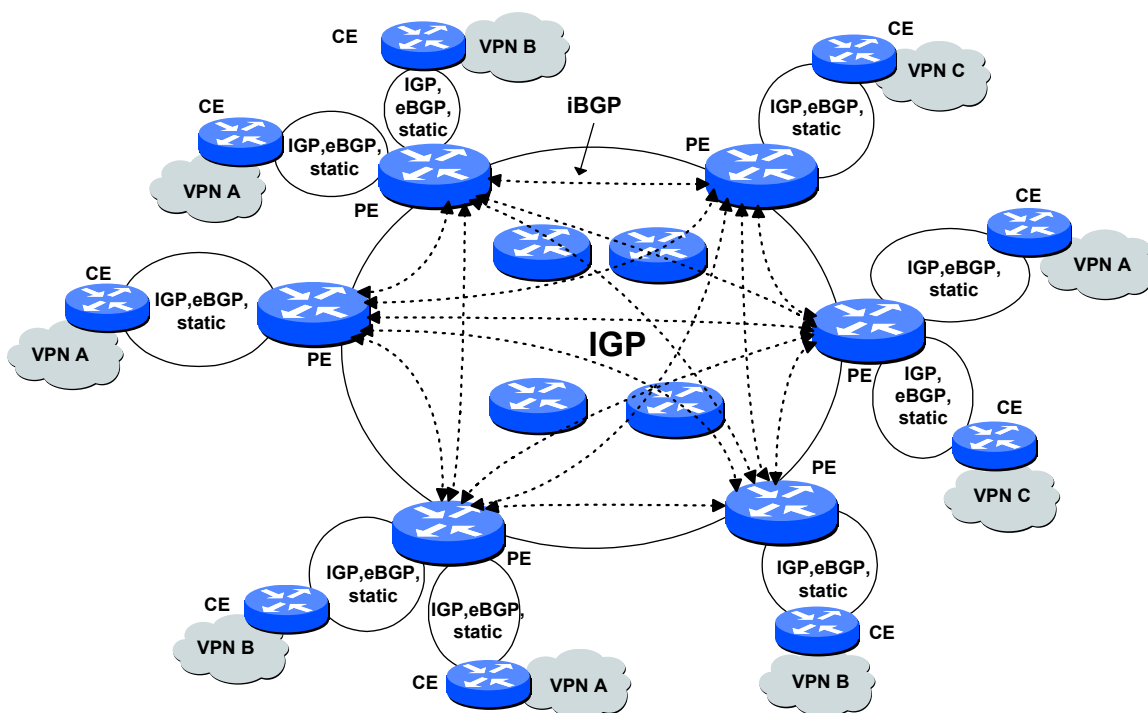
Na páteři sítě poskytovatele služeb je provozován IGP (*Interior Gateway Protocol*), např. OSPF, IS-IS nebo EIGRP, který dynamicky hledá optimální cesty v páteřní síti. Na základě směrovacích tabulek IGP, dojde k výměně MPLS značek mezi sousedícími zařízeními.

Směrování na rozhraní CE – PE

Na rozhraní se zákaznickou sítí je potřeba provádět výměnu lokálních směrovacích informací. Opět je vhodné použít některý z IGP, statickou cestu, případně BGP.

Výměna směrovacích informací mezi lokalitami

Aby byla zajištěna vzájemná bezpečnost provozovaných VPN, je potřeba provádět mezi jednotlivými PE směrovači na okraji MPLS sítě kontrolovanou distribuci cest do a z jednotlivých VPN. K tomuto účelu lze s výhodou využít směrovací protokol BGP (*Multi-protocol extension BGP*).



Obrázek 3-7 Směrování v MPLS síti poskytovatele služeb

IGP směrovací protokol provozovaný v páteřní síti je nezávislý na směrovacích protokolech provozovaných na spojnicích se zákaznickými sítěmi. V PE směrovačích nejsou informace příslušející k těmto nezávislým směrovacím procesům vzájemně redistribuovány.

Vhodnou filtrací BGP protokolu provozovaného na páteři sítě dosáhneme požadovaného zabezpečení vzájemné komunikace jednotlivých VPN sítí.

Při nasazení v síti velkého rozsahu je vhodné při implementaci BGP v páteři sítě zvolit jeden nebo několik PE směrovačů jako tzv. BGP Route Reflectors, které zajistí distribuci směrovacích informací k ostatním BGP partnerům (PE směrovačům). Vyhneme se provozování BGP komunikace mezi všemi PE směrovači navzájem.

Bezpečnost implementace VPN v prostředí MPLS sítě

Sítě využívající technologii MPLS poskytují úroveň zabezpečení shodnou se zabezpečením na druhé vrstvě OSI modelu (linková vrstva).

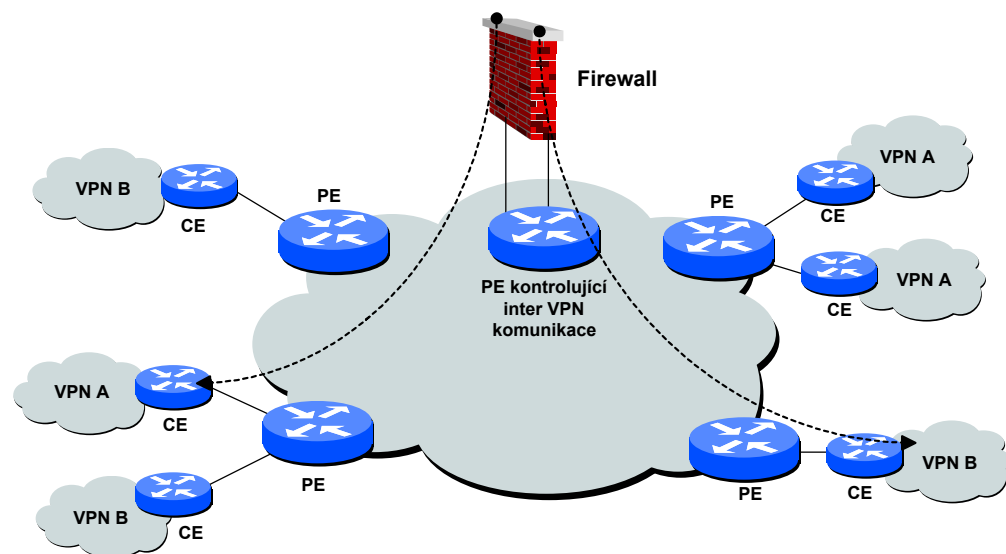
Při budování VPN sítí s využitím technologií ATM nebo Frame Relay jsou sítě vzájemně odděleny pomocí virtuálních kanálů (2. vrstva OSI).

Při nasazení technologie MPLS dochází k budování virtuálních sítí nad 3. vrstvou OSI modelu (oddělení na 3. vrstvě OSI modelu), ale vzhledem k principům technologie je úroveň zabezpečení shodná jako na 2. vrstvě, neboť lze zaručit nezávislou funkci jednotlivých virtuálních sítí na 3. a vyšší vrstvě na společném médiu.

- BGP protokol distribuuje směrovací informace o lokalitách VPN sítí jen ke zbývajícím členům dané VPN.
- Data jsou v síti přeposílána na základě LSP (*Label Switched Path*) definované staticky. Jde o stejný princip jaký nalezneme u technologií Frame Relay a ATM.
- Poskytovatel asociuje určitou VPN s určitým rozhraním na svém zařízení.
- Uživatelé mohou participovat v určité VPN, pouze když jsou připojeni ke správnému fyzickému portu a jejich pakety mají správnou VPN značku (*Route Distinguisher*).
- Datový provoz v jednotlivých VPN sítích je oddělen pomocí logicky nezávislých a oddělených směrovacích tabulek jedinečných pro každou VPN. Na základě vstupního portu je zvolena odpovídající směrovací tabulka, která obsahuje pouze destinace platné pro danou VPN (výsledek distribuce cest pomocí BGP protokolu).

Vzájemná komunikace mezi VPN sítěmi rozprostřenými přes páteřní MPLS infrastrukturu musí probíhat na základě přesných pravidel. Bezpečnostní ověřování mohou probíhat např. na specializovaném firewallu.

Následující obrázek ukazuje možnost bezpečné komunikace obecných VPN sítí.



Obrázek 3-8 Inter-VPN komunikace kontrolovaná firewallem

3.2. Výběr technologie pro rozlehlou síť ROWANet

Po důkladném rozboru požadavků zadavatele týkajících se možnosti bezpečného připojování jiných organizací k síti ROWANet doporučujeme pro tento účel využít technologii MPLS nebo VLAN over Gigabit.Ethernet.

Výhody nasazení technologie MPLS v síti ROWANet:

- rozšiřitelnost,
- podpora standardů,
- možná podpora QoS (*SLA compliance*),
- podpora správy datových toků (*traffic engineering*),
- přehlednost údržby a správy celé rozlehlé sítě,
- možnost připojovat síť s překryvným adresním schématem,
- celá síť je od počátku koncepčně připravena pro nasazení VPN a připojování VPN nevyžaduje složité rekonfigurace celé sítě,
- nižší ekonomická náročnost než v případě oddělení virtuálních sítí na druhé vrstvě OSI (FR, ATM).

Posledně zmíněná výhoda nižší ekonomické náročnosti (v porovnání s FR a ATM) vyplývá z těchto faktů:

- vyšší cena hardwarového vybavení potřebného pro vybudování sítě s možností oddělitelnosti VPN na 2. vrstvě OSI (nutnost vybavit všechny sítě ROWANet kromě směrovačů i Frame Relay přepínači) – odhadujeme o třetinu vyšší náklady,
- vyšší nároky na odborný obsluhující personál (náklady na speciální školení apod.).

Nevýhody nasazení technologie MPLS v síti ROWANet:

- nároky na odborný obsluhující personál – technologie využívá několika technologických stavebních prvků (BGP, IGP, MPLS, QoS).
- vyšší cena zejména softwarového vybavení proti variantě VLAN,
- složitější implementace proti variantě VLAN

Výhody nasazení technologie VLAN over GE v síti ROWANet:

- nejnižší ekonomická náročnost ze všech variant
- při výběru vhodného hardware možnost upgrade na MPLS VPN
- oddělení jednotlivých VPN na druhé vrstvě OSI modelu

Nevýhody nasazení technologie VLAN over GE v síti ROWANet:

- nutnost nekondfliktního adresního plánu
- problematické nasazení QoS,
- problematické zaručení přenosové kapacity v rámci jednoho trunku
- veškeré směrování mezi jednotlivými VLAN provádí pouze centrální L3 přepínač, včetně filtrace paketů z čehož plyne požadavek na velmi výkonný hardware (nejlépe Cisco Catalyst řady 6500)

Rozlehlost plánované sítě ROWANet a požadavky na připojování nezávislých subjektů do této sítě přesně zapadají do koncepce a oblasti doporučeného použití moderní technologie MPLS.

Aby však bylo možné plně využít předností nabízených MPLS technologií, je třeba použít fyzickou topologii typu kruh. V současné době je však plánována fyzická topologie typu hvězda, kde nelze plně využít všech předností MPLS technologie, a proto se nám jeví vhodnější a zároveň ekonomičtější využít technologii VLAN over Gigabit.Ethernet a zvolit vhodný hardware umožňující, v případě potřeby, budoucí upgrade na variantu MPLS VPN při zachování stávajících investic.

3.3. Infrastruktura a topologie

3.3.1. Základní principy návrhu topologie WAN sítě ROWANet

Pro budování sítě WAN je obecně nejlepší použít hierarchický model.

3.3.1.1. Hierarchický model

Hierarchický model navrhuje komunikační síť ve vrstvách. Stejný princip je použit v modelu vrstvené architektury ISO/OSI, který usnadňuje pochopení a realizaci komunikace počítačů. Idea zjednodušení spočívá v tom, že každá vrstva realizuje určité komunikační funkce. Návrhář sítě tak může v každé vrstvě vybrat nejlepší systémy a jejich vlastnosti.

Hierarchický systém dále usnadňuje změny. Modularita v návrhu umožní replikaci částí sítě tak, jak je třeba síť rozšiřovat. Změny sítě jsou přitom omezeny na malou část sítě (z toho vyplývají malé náklady a složitost provedení změny). Změny v sítích s plochou nebo plnou topologií mají tendenci ovlivnit větší část sítě.

Hierarchickou strukturu mají, či vyžadují rovněž další podpůrné technologie (rychlá konvergence směrovacích protokolů, sumarizace směrovacích cest, jmenový model). Hierarchický model je zpravidla strukturován do tří vrstev:

- **jádro** - poskytuje optimální transportní strukturu mezi lokalitami sítě,
- **distribuční vrstva** - poskytuje řízenou konektivitu lokalit sítě,
- **přístupová vrstva** - poskytuje přístup pracovním skupinám/uživatelům do sítě.

Každá vrstva představuje potřebnou funkčnost sítě. Vrstvy přitom nemusí být realizovány jako oddělené entity, mohou být realizovány v přepínačích nebo směrovačích, spoji či dokonce v jednom zařízení.

Jádro je vysokorychlostní páteř sítě. S její funkčností stojí a padá funkčnost celé sítě. Musí tedy být spolehlivá, redundantní a odolná vůči poruchám. K dalším požadavkům patří snadná správa, malé zpoždění a tudíž by měly být náročné manipulace s pakety (filtrování a jiné procesy) v této vrstvě vyloučeny.

Jádro sítě by rovněž mělo mít omezený průměr, který by se neměl měnit v závislosti na distribuční vrstvě. Omezení průměru sítě rovněž zajistí předvídatelnou výkonnost a usnadní odstraňování potíží (trouble-shooting).

Distribuční vrstva tvoří demarkační linii mezi přístupovou vrstvou a jádrem sítě. V této vrstvě mohou být realizovány mnohé funkce:

- bezpečnostní politika,
- agregace adres a oblastí,
- přechod na jiné spojové médium,
- redistribuce mezi směrovacími doménami,
- oddělovací hranice mezi statickými a dynamickými směrovacími protokoly.

Přístupová vrstva zajišťuje uživatelům, kteří jsou připojeni k lokálním segmentům, přístup do sítě. Pro pobočky, mobilní a vzdálené uživatele je typickou přístupovou vrstvou spoj rozlehlé sítě, využívající vlastní či pronajatý pevný datový okruh nebo ISDN.

3.3.2. Topologie páteřní sítě

Páteřní sítě by mohly být propojeny například všechna bývalá okresní města kraje Vysočina, případně další významná města v kraji, u nichž se dají předpokládat vysoké požadavky na přenosovou kapacitu.

Nejvíce používanými topologiemi jsou neredundantní topologie **Hub and Spoke** a redundantní **Ring** nebo **Multi ring**.

Výběr měst v příkladech topologie nemusí odpovídat skutečným potřebám a možnostem kraje Vysočina.

3.3.2.1. Hub and Spoke

Možné řešení topologie **Hub and Spoke** je zobrazen na následujícím obrázku.



Obrázek 3-9 Příklad topologie Hub and Spoke na páteři WAN

3.3.2.2. Ring

Možné řešení topologie **Ring** je zobrazeno na následujícím obrázku.



Obrázek 3-10 Příklad topologie Ring na páteři WAN

3.3.2.3. Multi ring

Možné řešení topologie **Multi ring** je zobrazeno na následujícím obrázku.



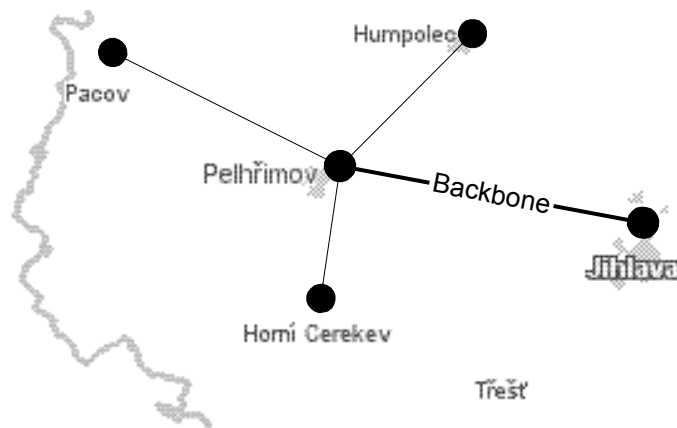
Obrázek 3-11 Příklad topologie Multi ring na páteři WAN

3.3.3. Distribuční vrstva

Stejně jako u topologií páteřní sítě jsou nejvíce používanými topologiemi neredundantní topologie **Hub and Spoke** a redundantní **Ring** nebo **Multi ring**.

3.3.3.1. Hub and Spoke

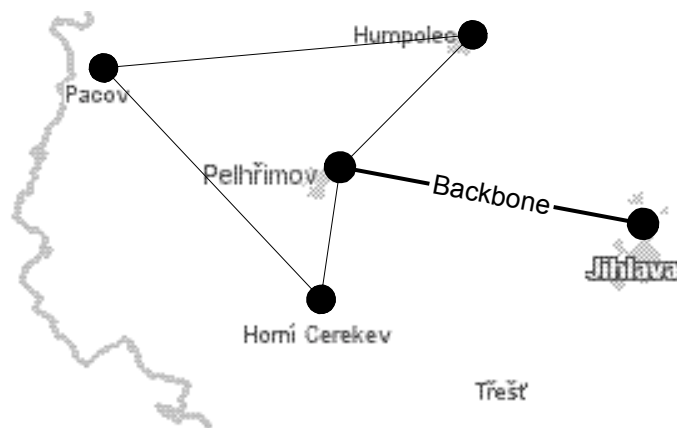
Možné řešení neredundantní topologie **Hub and Spoke** na distribuční vrstvě je zobrazeno na následujícím obrázku.



Obrázek 3-12 Příklad topologie Hub and Spoke na distribuční vrstvě

3.3.3.2. Ring

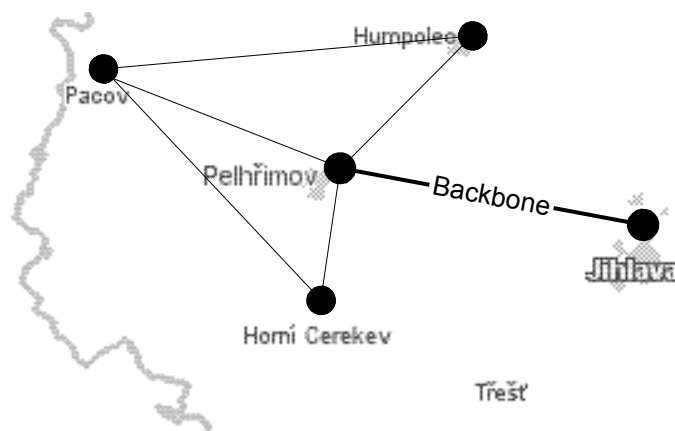
Možné řešení redundantní topologie **Ring** na distribuční vrstvě je zobrazeno na následujícím obrázku.



Obrázek 3-13 Příklad topologie Ring na distribuční vrstvě WAN

3.3.3.3. Multi ring

Možné řešení redundantní topologie **Multi ring** na distribuční vrstvě je zobrazeno na následujícím obrázku.



Obrázek 3-14 Příklad topologie Multi ring na distribuční vrstvě WAN

3.3.4. Přístupová vrstva

Přístupová vrstva se týká připojení jednotlivých subjektů v dané lokalitě k distribučnímu bodu.

Zde je opět možné použít topologie Hub and Spoke, Ring nebo Multi ring.

Většina subjektů pravděpodobně využije spoj point-to-point (topologie Hub and Spoke) k distribučnímu bodu ROWANetu, případně bude mít k dispozici z důvodu redundance ještě záložní linku k témuž bodu.

3.3.5. Redundantní topologie

Jsou-li v síti provozovány kritické aplikace, systémy, služby nebo spoje, je třeba při návrhu sítě určit pravděpodobnost výpadku kritické komponenty a bránit se zavedením patřičné redundance.

Obecně rozeznáváme redundanci:

- směrovačů,
- serverů,
- směrovacích cest,
- fyzických spojů.

V praktických případech se používá redundance směrovačů v jádru komunikační sítě, serverů v datových centrech a částečné redundance cest.

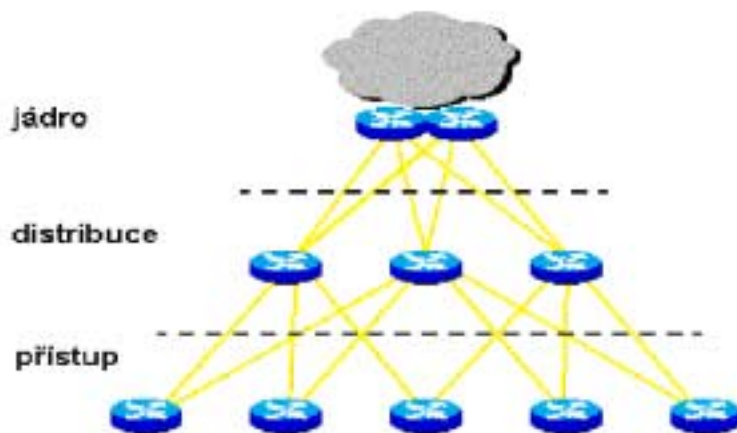
V některých prostředích, kdy je nutné zajistit nepřetržitou dostupnost dat, je třeba zajistit plnou **redundanci datových serverů**. To v důsledku vede ke koncepci plně redundantních datových center (pro jednoduchost a s ohledem na ekonomická hlediska předpokládáme dvě taková centra). Tato centra pak musí být umístěna na různých segmentech sítě, na různých zdrojích napájení a nejlépe v různých lokalitách (v extrémním případě městech). Dalším nezbytným požadavkem je konektivita obou datových center vysokorychlostními spoji a těmi síťovými protokoly, které se k replikaci dat a pro přístup k datům používají, resp. používat budou.

Zde je třeba ještě rozlišit význam pojmů „datové“ a „komunikační“ centrum. Datové centrum si lze představit jako zařízení shromažďující data, například databázový server. Komunikační centrum představuje centrální uzel sítě, nebo-li také vrchol topologického stromu sítě. Redundance komunikačního centra (centrálního uzlu sítě) nevyžaduje nutně redundanci datových center (databázových serverů) a naopak. Lze proto budovat síť s jedním komunikačním centrem a několika redundantními datovými centry nebo síť s několika komunikačními centry a jedním centrem datovým. Při budování sítí se doporučuje nejdříve zabezpečit permanentní konektivitu prostřednictvím redundance komunikačních center a spojnic a následně (pokud je to nutné) zabezpečit permanentní přísun dat také redundancí datových center.

Návrh **redundantních směrovacích cest** si klade dva cíle:

- rozložení zátěže,
- minimalizace výpadků (downtime).

Redundantní cesty přispívají k minimalizaci výpadků tím, že výpadek jednoho spoje neovlivní chod sítě katastrofálním způsobem. Extrémním případem redundance cest je tzv. úplná topologie, kdy existuje spoj mezi každými dvěma uzly sítě. Počet spojů je $n \cdot (n-1) / 2$, kde n je počet uzlů, proto počet spojů rychle narůstá s počtem uzlů a je tedy provozně náročnou topologií. Proto se zpravidla při návrhu vychází z hierarchického návrhu topologie, v němž se uplatní jistá omezená redundance cest.

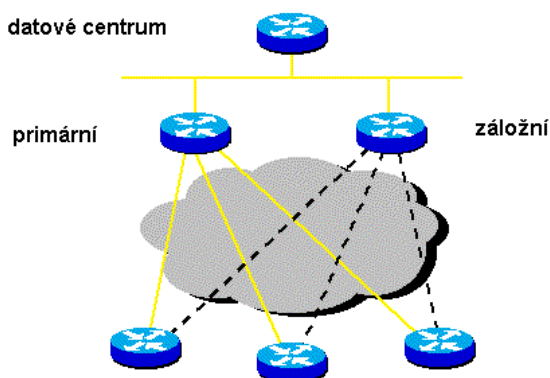


Obrázek 3-15 Příklad částečné redundance cest

Redundance cesty je v tomto případě dvojnásobná v každé vrstvě se zachováním stejné šířky pásma a tudíž i metriky.

O **redundanci fyzických spojů** mluvíme v případě, že jeden spoj mezi dvěma lokalitami je realizován alespoň dvěma nezávislými způsoby. Je přitom důležité, aby fyzické spoje byly na sobě opravdu nezávislé, např. procházely jinými technologickými kanály, byly poskytovány jinou infrastrukturou resp. poskytovatelem, byly založeny na jiném fyzikálním principu atd.

Redundance fyzických spojů v prostředí WAN je citlivá záležitost, neboť redundantní topologie je drahá. Jde-li např. o přístup do datového centra, jak je naznačeno na následujícím obrázku, pak se zpravidla používá jeden primární fyzický spoj a jeden záložní.



Obrázek 3-16 Redundance fyzických spojů

Záložní spoj je aktivován (a platí se za něj) jen v případě výpadku primárního fyzického spoje, nebo když je primární spoj přetížen.

Pro aktivaci záložního spoje při výpadku primárního spoje lze např. využít vysoké administrativní vzdálenosti záložní cesty. Při normálním provozu primárního spoje tedy směrovací algoritmus nikdy záložní spoj nevybere.

Obvykle se pro primární fyzické spoje využívají pronajaté datové okruhy, avšak v případě WAN sítě kraje Vysočina připadají v úvahu vlastní optické okruhy v kombinaci s pronajatými. Jako záložní infrastruktura připadají v úvahu sekundární optické okruhy, pronajaté okruhy, satelitní spoje.

V případě přístupové vrstvy, pokud se spokojíme s nižší propustností, lze využít ISDN. Je-li pro záložní spoje využita ISDN, pak při výpadku primárního spoje dojde k automatickému ustavení záložního ISDN spoje.

V případě použití redundance fyzických přenosových cest v páteřní vrstvě rozlehlé sítě je nutná také realizace redundantních komunikačních center ve vrcholu topologického stromu.

3.4. Přenosová infrastruktura WAN sítě ROWANet

Jedním ze základních aspektů, které je třeba posuzovat při celkovém návrhu komunikační sítě, je i návrh přenosového prostředí. V úvodu této kapitoly je tedy uveden přehled vhodných komunikačních technologií, které mohou být obecně použity při budování WAN sítě ROWANet a v dalších částech je pak návrh přenosových prostředí pro jednotlivé topologické celky navrhované WAN sítě (páteřní vrstva, distribuční vrstva, přístupová vrstva).

3.4.1. Přehled komunikačních technologií

3.4.1.1. Okruhy na bázi optických vláken

Nejvhodnější technologií pro budování **primární přenosové infrastruktury** páteřní a distribuční vrstvy sítě ROWANet se jeví přenosové technologie na bázi optických vláken.

Optická vlákna sdružená do optických kabelů nabízejí oproti dalším přenosovým technologiím nesrovnatelnou přenosovou kapacitu, spolehlivost a bezpečnost. Nad optickými vlákny je možné provozovat např. některý z následujících protokolů nebo transportních systémů: SDH/SONET, Packet over Sonet, Ethernet (Gigabit Ethernet), ATM (Asynchronous Transfer Mode), SAN (Storage Area Network), FiberChannel, DPT (Dynamic Packet Transport).

Pro případné další zvýšení přenosové kapacity může být využita technologie **vlnového multiplexu** (dělení).

Vlnové dělení (WDM, Wavelength Division Multiplexing) umožňuje multiplexovat optické signály pracující na různých vlnových délkách, a tak je přenášet paralelně po optickém vlákně. Tak každá z vlnových délek poskytuje šířku pásma dosud nabízenou celým jedním optickým vláknem.

WDM je zcela transparentní vůči přenášeným protokolům. S WDM může každá vlnová délka přenášet uživatelský provoz o různé rychlosti a v různém formátu (SONET/SDH, Ethernet, ATM, Asynchronous Transfer Mode, SAN, Storage Area Network, FibreChannel, DPT, Dynamic Packet Transport), a tak se zvyšuje využitelná šířka pásma optického vlákna i využitelnost pro různé služby. Před WDM jedno vlákno mohlo podporovat pouze jediný kanál SONET/SDH (Synchronous Optical Network/Synchronous Digital Hierarchy) nebo gigabitového ethernetu. Dnes existuje řada komerčních optických sítí, které podporují na jednom optickém vlákně jak signály typu SONET o rychlosti 2,5 Gbit/s (OC-48c), tak signály o rychlosti 10 Gbit/s (OC-192).

Optické přepínače jsou dnes schopny podporovat 256 vlnových kanálů, každý z nich o rychlosti 10 Gbit/s (OC-192), takže dosahují agregované rychlosti v řádu Tbit/s.

Pro páteřní vrstvu sítě ROWANet a v místech kde to bude možné i pro distribuční vrstvu navrhujeme využít protokolu Gigabit Ethernet nad optickou infrastrukturou.

Tato infrastruktura může být buď vlastní nebo pronajatá v těch místech, kde již nějaká optická infrastruktura již existuje a její pronájem bude ekonomicky výhodnější, než budovat vlastní optické trasy.

Možnosti pronájmu optické infrastruktury jsou následující:

- **Dark fiber** - zákazník si pronajme 1 "nenasvícené" optické vlákno:
 - musí si sám instalovat vše potřebné pro "nasvícení" vlákna (zdroj světla, detektor),
 - má k dispozici celou přenosovou kapacitu vlákna, může si sám realizovat WDM.
- **Pronájem barvy** - zákazník si pronajímá přenosové schopnosti 1 přenosového kanálu (barvy):
 - jako obdobu 2bodového spoje, s konstantní (vyhrazenou) přenosovou kapacitou,
 - může (musí) si sám zvolit přenosové protokoly (SDH/SONET, ATM, IP, ...).
- **Protokolová konektivita** - konektivita na úrovni protokolu IP nebo jiného protokolu:
 - ATM, SDH, ...
 - Realizaci protokolu zajišťuje provozovatel sítě.

V případě pronájmu optické infrastruktury pro síť ROWANet doporučujeme pronájem typu „**dark fiber**“ nebo případně „**pronájem barvy**“ s využitím technologií WDM (CWDM, DWDM), která umožňuje budování MPLS páteřní sítě.

3.4.1.2. Pevné pronajaté okruhy

Charakteristickým rysem **pevných pronajatých okruhů** je realizace dvoubodových spojení se synchronním přenosem dat. Vlastní komunikace je pak řízena příslušným protokolem, například PPP, HDLC apod.

Velkou **výhodou** pronajatých okruhů je to, že každý spoj má trvale přidělenou přenosovou šířku pásma s konstantním zpožděním. Pronajaté okruhy jsou tedy ideální platformou pro implementaci multifunkčních komunikačních sítí s prostředím TCP/IP, které integrují datové komunikace s komunikacemi hlasovými, faxovými a obrazovými (přenos videosignálu).

Další výhodou komunikace nad pronajatými okruhy je:

- Efektivní využití přenosové kapacity, což je dáno vysokou efektivností linkových protokolů pro synchronní komunikaci a jejich relativní jednoduchostí, která umožňuje přenést jejich zpracování až na úroveň hardwaru.
- Velký výběr komunikačních protokolů, které je možné využít pro realizaci spojení po pevném pronajatém okruhu (PPP, HDLC, LAPB apod.). Vhodnou volbou linkového protokolu pro dané datové linky lze zvýšit efektivnost využití přenosových prostředků, aplikovat autentizační protokoly jako prostředky pro technologickou ochranu sítě, v případě potřeby lze data přenášená po pevném pronajatém okruhu snadno šifrovat apod.
- Možnost použití nejrůznějších kompresních technik, které umožní ještě efektivnější využití kapacity linky.

Technologii **pevných pronajatých okruhů** je vhodné použít jako **druhou nejvhodnější** pro implementaci **primární přenosové infrastruktury** páteřní a distribuční vrstvy WAN sítě ROWANet a to zejména tam, kde není možné použít vlastní či pronajatá optická vlákna.

Na přístupové vrstvě je technologie pevných pronajatých okruhů vhodná pro vysokorychlostní připojení vybraných lokalit.

3.4.1.3. Technologie Frame Relay

Frame Relay patří k technologiím používajícím ke komunikaci principu přepínání paketů a řadí se mezi spojově orientované komunikační technologie. Rozhraní, jímž se připojují koncová zařízení k síti Frame Relay, používá techniky statistického multiplexingu více virtuálních kanálů přes jedno fyzické rozhraní.

Virtuální kanály u Frame Relay jsou identifikátory sestaveného spojení mezi dvěma koncovými zařízeními. Toto virtuální spojení je obousměrné a do jednoho fyzického okruhu lze mapovat více okruhů virtuálních. Virtuální okruhy se dělí na dva typy - **SVC (Switched Virtual Circuit)** a **PVC (Permanent Virtual Circuit)**. SVC okruhy se používají k nahodilému přenosu dat a podléhají procesu sestavování a rušení. PVC okruhy jsou mezi koncovými zařízeními sestaveny stále a používají se ke kontinuálnímu přenosu dat mezi koncovými zařízeními.

Virtuální okruhy jsou identifikovány pomocí identifikátoru **DLCI (Data Link Connection Identifier)**. DLCI je zpravidla přidělován poskytovatelem Frame Relay sítě a má lokální význam. Jedním ze základních parametrů, který je nutno specifikovat v okamžiku objednání služby je tzv. **parametr CIR (Committed Information Rate)**. Tento parametr udává „rychlost“ v kilobitech za sekundu, se kterou jsou rámce za normálních podmínek přenášeny sítí, a která je provozovatelem sítě garantována (committed). Parametr CIR představuje „průměrnou“ zaručenou minimální propustnost v síti a jeho správné nastavení je klíčovým momentem pro ekonomický a zároveň dostatečně nadimenzovaný návrh síťového řešení. Druhým důležitým parametrem, který nastavuje provozovatel sítě je tzv. parametr **EIR (Excess Information Rate)**. EIR udává rychlost přenosu rámců v kilobitech za sekundu, o kterou je možno za normálních podmínek (je-li v síti k dispozici potřebná přenosová kapacita) překročit hodnotu parametru CIR. Celková přenosová rychlost dosahuje potom hodnoty CIR + EIR.

Technologie Frame Relay je vhodným řešením pro potřeby rychlého přenosu a zpracování dat s nárazovým charakterem, kterému typicky odpovídá komunikace LAN-to-LAN, která není **citlivá na proměnné zpoždění**. Proměnné zpoždění má však velký vliv například na **kvalitu přenášeného hlasového signálu**.

Proměnlivost zpoždění je významným faktorem především u veřejných datových sítí, které negarantují konstantní dobu zpoždění přenosu informačního rámce (neposkytují tzv. služby **Quality of Service**). Doba zpoždění přenosu informačního rámce je závislá na aktuálním zatížení Frame Relay sítě, která v případě svého přetížení přenášené rámce buď ukládá ve vyrovnávacích bufferech FR přepínačů nebo je přímo vyřazuje.

Vzhledem k tomu, že **není známo**, zda jedním z požadavků zadání budování WAN sítě **ROWANet** nebude i **integrace hlasových a video přenosů**, **nelze** použití veřejné sítě Frame Relay jako přenosového prostředí WAN ROWANet z výše uvedených důvodů **doporučit**.

3.4.1.4. Technologie ATM

Technologie ATM umožňuje integrovat datové přenosy s hlasovými a obrazovými (citlivými na zpoždění) a lze s její pomocí vytvářet skutečné multifunkční sítě s vysokými přenosovými kapacitami (až 2,48 Gbit/s). Další standardizační vývoj a zájem výrobců a poskytovatelů přenosových služeb o tuto technologii ji předurčuje k dlouhému životu, dlouhodobému rozvoji a širokému nasazení ve všech oblastech datových i nedatových (multimediálních) aplikací.

ATM síť může účastníkům zprostředkovat dva různé typy spojení:

- SVC (Switched Virtual Circuit) - spojení dynamicky navazované koncovými zařízeními navzájem s možností specifikace QoS.
- PVC (Permanent Virtual Circuit) - spojení předkonfigurovaná administrátorem ATM sítě, opět s možností specifikace QoS.

Protokoly síťové vrstvy (např. IP) je pak možné přenášet sítě ATM po spojeních typu SVC nebo PVC.

Spojení SVC jsou v ATM síti vytvářena prostřednictvím signalizačních protokolů, které jsou součástí definice síťových rozhraní.

Spojení PVC jsou v síti ATM definovány staticky administrátorem sítě, a to tak, že identifikátory tohoto spojení je nutno definovat na všech ATM přepínačích, které jsou v cestě mezi spojovanými koncovými uzly.

Uvedené typy virtuálních okruhů mohou mít charakter buď dvoubodových spojení (point-to-point PVC nebo SVC), nebo vícebodových spojení (point-to-multipoint PVC nebo SVC).

Technologie **ATM** může být v navrhované síti **ROWANet** použita jako **jedna z alternativních přenosových technologií**, například pro propojování komunikačních uzlů budované sítě prostřednictvím ATM infrastruktury metropolitních sítí, případně pro realizaci páteřních spojů (tam, kde by to bylo cenově výhodné).

3.4.1.5. Technologie ISDN

Technologie ISDN (Integrated Services Digital Network) je technologie, která umožňuje cenově efektivní integrovaný přenos hlasu a dat. K výhodám technologie ISDN patří především to, že je **digitální technologií**, která se vyznačuje **malou chybovostí** a celkově **vyšší spolehlivostí** oproti klasickým analogovým technologiím.

Základním prvkem architektury ISDN je kanál s přenosovou rychlostí 64 kbit/s, který je pro uživatele plně transparentní, neboť jedním z výchozích principů filosofie ISDN bylo oddělení signalizace od užitečných dat (Out-of-Band signaling). Tento kanál je označován jako B-kanál. Pro signalizaci je vyhrazen zvláštní kanál s rychlostí 16 nebo 64 kbit/s, tzv. D-kanál. Ten je společný pro všechny B-kanály dané přípojky. Počet B-kanálů a rychlost D-kanálu je dána typem přípojky do sítě ISDN. K dispozici jsou dva hlavní typy rozhraní - BRI a PRI. BRI přípojka poskytuje uživateli 2 B-kanály a 1 D-kanál s rychlostí 16 kbit/s (označuje se též jako 2B+D). Pro tento typ přípojek se využívají stávající dvoudrátová účastnická vedení používaná standardně pro analogové přípojky. PRI přípojka obsahuje v evropské verzi 30 B-kanálů a 1 D-kanál o rychlosti 64 kbit/s. Přípojná vedení pro tuto přípojku jsou „čtyřdrátová“ a pro každý směr přenosu je vyhrazen zvláštní pár.

Digitální síť integrovaných služeb lze charakterizovat těmito parametry:

- V síti se pracuje s digitálními kanály s přenosovou rychlostí 64 kbit/s; ISDN je koncipována jako síť s komutací okruhu, umožňuje však i přenos zpráv s komutací paketu.
- Účastnické přípojky ISDN pracují s tzv. základním přístupem 2 B+D, kde se po dvoudrátovém účastnickém vedení realizují dva obousměrné informační kanály B, každý s přenosovou rychlostí 64 kbit/s, a obousměrný signalizační kanál D s přenosovou rychlostí 16 kbit/s. Každý z informačních kanálů B může být využit pro jednu službu. Obě služby mohou probíhat současně a spojení mohou být uskutečněna se dvěma různými účastnickými přípojkami.
- Střední a velké pobočkové ústředny ISDN se připojují primárním přístupem 30 B+D, který obsahuje 30 obousměrných informačních kanálů B, každý s přenosovou rychlostí 64 kbit/s, a jeden signalizační kanál D s přenosovou rychlostí 64 kbit/s.
- Každá účastnická přípojka ISDN má v ústředně ISDN přidělené jedno přípojně číslo bez ohledu na počet připojených koncových zařízení. Výběr jednoho z koncových zařízení, které odpovídá dané službě, se uskutečňuje na základě informace přenášené v signalizačním kanálu D.
- Stávající ISDN sítě, které pracují s digitálními kanály 64 kbit/s, se označují jako úzkopásmové (NISDN - Narrowband ISDN). Na účastnické přípojce lze použít již existující dvoudrátové přípojně vedení, telefonní přípojku.
- V úzkopásmové ISDN lze přenášet v digitálním tvaru kromě zpráv hlasových telefonních spojení, textových a datových také statické nebo pomalu se pohybující obrazy.

Z hlediska komunikačních sítí lze základní aplikace ISDN rozdělit na:

- **Primary line backup** - cenově efektivní záloha primárního spojení (např. pevná linka, Frame Relay spojení apod.).
- **Dial-on-demand** - směrovač pobočky nemá dedikované spojení na centrální lokalitu. Pokud je potřeba přenést data, je sestaveno spojení a pokud nejsou data přenášena po definovanou dobu, spojení je ukončeno.
- **Dial-on-congestion** - umožňuje zvýšit propustnost primárního spoje v případě, že jeho kapacita nedostačuje (např. v určitou denní dobu).

Použití přenosové infrastruktury ISDN je cenově výhodné tam, kde není třeba stálého spojení prvků sítě, které se nacházejí ve dvou odlehlých lokalitách. Například u aplikací typu klient-server. Na základě provedených studií bylo zjištěno, že výhodnost přenosové infrastruktury ISDN je prokazatelná u spojnic, jejichž doba použití (celková doba navázaného spojení) je menší než asi 3,5 hodiny denně v pracovní dny. V dobu mimo pracovní dny se nepředpokládá žádný datový provoz na těchto linkách. Překročí-li doba navázaného spojení výše zmíněnou hodnotu, je výhodnější použít pevnou linku.

V navrhované WAN síti **ROWANet** doporučujeme tuto technologii použít pro realizaci vybraných **primárních nebo záložních spojů** na úrovni **přístupové** vrstvy, které splňují výše uvedenou podmínku, připojení kratšího než 3,5 hod/den a nemožnosti jiného alternativního, cenově výhodnějšího připojení (např. wi-fi, FWA 26 GHz).

3.4.1.6. FWA 26 GHz

FWA (Fixed Wireless Access) je bezdrátová technologie určená pro budování přístupových komunikačních sítí na principu Point-to-Multipoint (P-MP). Umožňuje alternativní řešení tzv. poslední míle.

Hlavním rysem této technologie je velká propustnost pásma, která nám umožňuje realizovat vysokorychlostní datové přenosy, hlasová spojení a provoz dalších telekomunikačních služeb. Tato technologie je licencovaná.

Technologii FWA 26 GHz lze doporučit jako vhodnou pro přístupovou vrstvu.

3.4.1.7. 802.11b/g

Bezdrátové síť **802.11b/g** lze **doporučit** jako jednu z **alternativních možností** pro přístupovou vrstvu WAN sítě **ROWANet**.

Je však třeba vyřešit **bezpečnostní** aspekty bezdrátového propojení sítí. Rádiové síť jsou již z principu své činnosti vystaveny jednak riziku odposlechu neautorizovanými osobami a jednak neautorizovanému přístupu. Proto je nutné s jejich nasazením implementovat i dostatečně silné bezpečnostní mechanismy (např. IPsec tunely).

Standard 802.11b využívá přenosovou metodu DSSS (Direct Sequence Spread Spectrum) a definuje maximální přenosovou bitovou rychlost 11 Mbit/s s možností snížení rychlosti na 5,5 Mbit/s, 2 Mbit/s a 1 Mbit/s. V ETSI (European Telecommunication Standards Institute) verzi standardu (ze které vychází i generální licence ČTÚ) je pro přenos vyhrazeno rádiové pásmo 2,4 – 2,4835 GHz, ve kterém je možné definovat 13 kanálů. Vzhledem ke spektrální šířce modulovaného kanálu je však možné umístit do vyhrazeného pásma maximálně tři kanály, které se vzájemně neruší. Z toho vyplývá, že při použití více jak tří přístupových bodů se musí tvarovat velikost (dosah) rádiových buněk tak, aby nedocházelo k jejich vzájemnému rušení. Podmínky provozování zařízení na území České republiky upravuje generální licence ČTÚ č. GL-12/R/2000.

IEEE 802.11g (Higher Speed Physical Layer (PHY) Extension to IEEE 802.11b), pracuje ve stejném bezlicenčním pásmu 2,4 GHz jako WiFi (802.11b), ovšem maximální rychlostí na fyzické vrstvě dosahující 54 Mbit/s (podobně jako u 802.11a). Obdobně jako 802.11b může podporovat maximálně tři nepřekrývající se kanály; podobnost je i v dosahu sítě (u stejných rychlostí, s vyššími rychlostmi dosah u 802.11g klesá až na 30 metrů). 802.11g je zpětně slučitelná s 802.11b, takže v jedné síti mohou pracovat klienti obou typů sítí. Obě specifikace se ovšem liší řešením fyzické vrstvy: WiFi používá DSSS a 802.11g OFDM (pro spolupráci s Wi-Fi navíc také DSSS).

3.4.2. Volba přenosové infrastruktury pro ROWANet - shrnutí

Na základě předchozího rozboru jednotlivých přenosových technologií lze v současné době jako perspektivní přenosové technologie pro realizaci přenosové infrastruktury v jednotlivých vrstvách navrhované WAN sítě ROWANet označit:

Páteří vrstva – pro implementaci **primárních komunikačních spojů** je nejvhodnější **technologie optických vláken** (vlastních či pronajatých). Tam, kde nelze použít technologii optických vláken, pro záložní spoje doporučujeme **technologie pronajatých digitálních okruhů**.

Distribuční vrstva – nejvhodnější je opět **technologie optických vláken**, případně **pronajatých digitálních okruhů**. V případě budování záložní infrastruktury opět doporučujeme využít technologii **pronajatých digitálních okruhů**.

Přístupová vrstva – v praxi lze pro tuto vrstvu využít v principu jakoukoli z výše uvedených technologií, v závislosti na požadované **přístupové rychlosti a dostupnosti v dané lokalitě**. Technologii **ISDN doporučujeme** pro implementaci **záložní přenosové infrastruktury**.

Uvedené přenosové technologie mohou být dále kombinovány všude tam, kde to bude cenově efektivní, s dalšími nevyjmenovanými přenosovými technologiemi. Jako příklad použití alternativní technologie lze označit např. realizaci komunikačních spojů budované sítě ROWANet prostřednictvím přenosových prostředků regionálních optických či ATM metropolitních sítí.

Pokud bude nutné do vybraných lokali donést více než jednu VPN, je vhodné vybrat tu technologii, která podporuje nativně přenos více navzájem oddělených VLAN. V případě, že nasazení takové technologie v dané lokalitě není možné, lze takovou situaci řešit pomocí šifrovaných IPsec tunelů.

3.4.3. Využití alternativních infrastruktur

Ke spojení distribučních uzlů ROWANetu a ostatních organizací může být využito některých alternativních přenosových infrastruktur. Jedná se například o spojení úřadů, které jsou lokalizovány v jednom městě a mohou tedy být propojeny prostřednictvím metropolitní sítě nebo jiné sítě. V takových případech doporučujeme postupovat individuálně dle samostatného projektu, protože technická jednotnost řešení konkrétních sítí v jednotlivých městech není zaručena.

Na modelovém případě obecné sítě představíme doporučovaný způsob propojení městských lokalit. Předpokládejme obecné přenosové prostředí modelové sítě (ATM, ATM LANE, Gigabit Ethernet apod.). V tomto přenosovém prostředí bude vytvořena topologie hub-and-spoke. Centrálním bodem této topologie bude lokalita regionálního ROWANetu.

Připojení tohoto uzlu k metropolitní síti je klíčové a mělo by být provedeno jako první. Krajními přípojnými body budou uzly komunikační uzly různých organizací.

V přenosovém prostředí metropolitní sítě budou vytvořeny spoje, které plně nahradí spoje typu bod-bod realizované prostřednictvím hlavních přenosových infrastruktur (Např. LLNet). Tyto spoje mohou být vytvořeny různými způsoby. Například pomocí technologie virtuálních okruhů, nebo pomocí tunelů.

Velkou pozornost je v tomto případě rovněž nutné věnovat bezpečnosti, zejména na úrovni rozhraní poskytovaného provozovatelem dané metropolitní sítě. Jako vhodné lze v tomto případě označit takové rozhraní, které podporuje konfiguraci nezávislých virtuálních okruhů (ATM, Frame Relay apod.) nebo rozhraní fyzické vrstvy (např. optický spoj). Z bezpečnostních důvodů je třeba zvážit použití rozhraní typu Ethernet, které je možné snadno „odposlouchávat“, zejména v případě, kdy administrátorem koncového zařízení metropolitní sítě je sám provozovatel metropolitní sítě.

V případě vyšších požadavků na zabezpečenou komunikaci a v případě, že bude nezbytné použít rozhraní typu Ethernet pro připojení do metropolitní sítě poskytovatele, doporučujeme data transportovaná nad takto vytvořeným komunikačním spojením šifrovat.

3.5. Výběr komunikačního protokolu a adresní plán

Způsob komunikace mezi koncovými zařízeními počítačové sítě (stanice, servery) je určen typem zvoleného komunikačního protokolu – pravidel komunikace. Komunikující koncová zařízení musí takový protokol podporovat. Existuje řada protokolových sad, některé méně, jiné více využívané v dnešních počítačových sítích (např. OSI, IPX/SPX, Decnet, AppleTalk, TCP/IP).

Architektura TCP/IP – Transport Control Protocol / Internet Protocol je stále *de facto* standardem a v současné době jde o nejpoužívanější architekturu pro budování datových sítí. Implementace TCP/IP jsou standardní součástí operačních systémů typu UNIX, Windows apod.

3.5.1. IPv4 versus IPv6

V současné době existuje možnost nasazení protokolu IPv6 ve WAN síti ROWANet. Protokol IPv6 má mnohé výhody proti protokolu IPv4 a také některé nevýhody.

Některé výhody IPv6:

- Významné rozšíření adresního prostoru.
- Efektivnější přenos dat.
- Podpora pro mobilní zařízení.
- Zabudovaná bezpečnost na bázi IPsecu.

Nevýhody IPv6:

- Zatím spíše pro „nadšence“.
- V současné době ještě ne zcela otestovaná technologie.
- Většina dnešních sítí (včetně Internetu) je provozována na bázi IPv4. Z toho plyne nutnost překlady IPv6 na IPv4 na hraničních směrovačích.

Vzhledem k současné nevyzrálosti implementace IPv6 a nutnosti překlady na IPv4 na směrovačích hraničících s připojovanými či transportovanými sítěmi, doporučujeme použít ve WAN síti **ROWANET** protokol **IPv4**.

Tento dokument se bude dále zabývat pouze protokolem IPv4.

3.5.2. Adresní plán

3.5.2.1. Základní principy adresního plánu

Na základě doporučení RFC 1918 navrhujeme zvolit pro adresaci nově budované sítě ROWANet privátní adresní rozsah třídy A 10.0.0.0 – 10.255.255.255. Takto zvolený rozsah adres pokrývá dostatečným způsobem současné i případné budoucí požadavky na velikost nebo i rozšiřování adresního prostoru.

Vzhledem k tomu, že síť ROWANet budou využívat různé organizace jako jsou KÚ Vysočina, úřady veřejné samosprávy, Hasičské záchranné sbory, školy a další nekomerční (případně i komerční) organizace, je pro připojované organizace vhodné definovat nezávislé adresní rozsahy v rámci zvolené adresy sítě 10.0.0.0. Tím bude usnadněna případná filtrace vzájemných komunikací a zajištěna nekonfliktnost s adresním plánem GOVBONE.

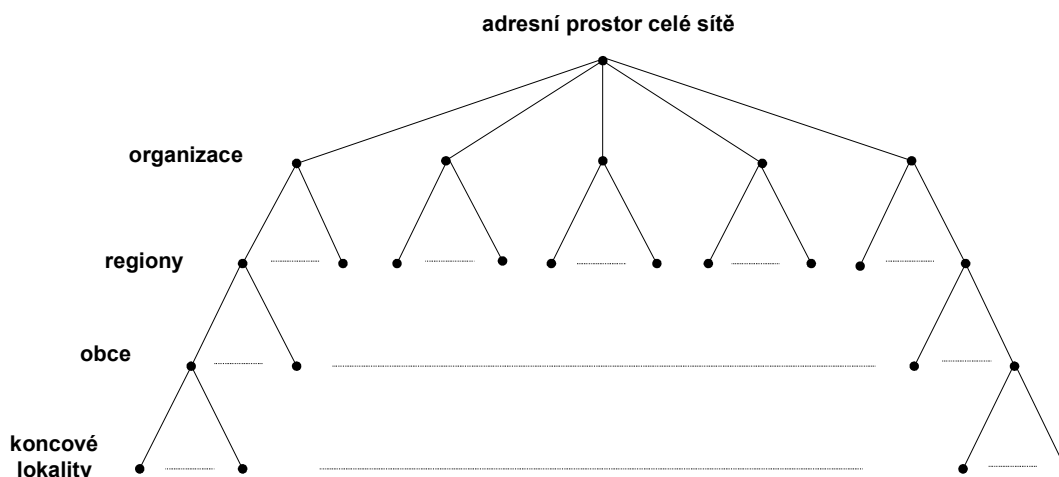
Navrhovaný adresní plán měl být zejména:

- rozšiřitelný,
- přehledný,
- flexibilní při případných změnách v topologii nebo směrovací strategii,
- respektující rozdělení na VÚSC (Vyšší územně správní celky).

Na základě těchto požadavků na vlastnosti adresního plánu navrhujeme rozdělit postupně zvolený adresní prostor dle:

- organizací,
- regionů,
- obcí,
- koncových lokalit.

Následující obrázek schématicky znázorňuje princip doporučeného hierarchického dělení adresního prostoru sítě ROWANet.



Obrázek 3-17 Hierarchické dělení adresního prostoru

Hierarchické dělení adresního prostoru usnadní konfiguraci směrovacích protokolů v síti ROWANet.

3.5.2.2. Technologie MPLS a překryvné adresní rozsahy

Technologie MPLS (*Multiprotocol Label Switching*) poskytuje možnost využít jedinou společnou komunikační infrastrukturu pro mnoho různých komunikačních sítí (virtuálních privátních sítí), přičemž je možné, aby adresní schémata těchto připojovaných (zákaznických) sítí nebyla navzájem disjunktní.

Není tedy potřeba provést přecíslování nově připojované sítě před připojením nové organizace k síti vybudované technologií MPLS.

Výhody jsou zejména ve velké pružnosti a rozšiřitelnosti takto vybudované komunikační infrastruktury.

Nevýhody spočívají v řešení problému v případě potřeby komunikace mezi VPN s překryvným adresním rozsahem.

3.5.2.3. Adresace v páteřní síti

Pro páteřní rozsah IP adres doporučujeme rezervovat blok velikosti třídy B na konci adresního rozsahu sítě 10.0.0.0, který bude odlišný od adres sítí přidělovaných připojovaným organizacím.

3.5.2.4. Adresace sítí připojovaných subjektů

Základním je dělení adresního prostoru na disjunktní prostory vyhrazené jednotlivým organizacím. Doporučujeme vyhradit každé organizaci 1 až 16 podsítí velikosti třídy B, dle velikosti dané organizace s přihlédnutím k jejím budoucím potřebám.

V případě organizací, které nemají a ani v budoucnu nepředpokládají potřebu mezi sebou komunikovat, lze přiřazovat nedisjunktní adresní prostory. Doporučujeme k tomuto kroku však přistoupit až po vypotřebování celého adresního rozsahu, vzhledem k nevýhodám, které tento postup přináší:

- Nemožnost vzájemné komunikace, bez nesystémových zásahů do sítě (např. NAT).
- Omezený přístup ke sdíleným zdrojům – zdroje musí mít adresy z veřejného rozsahu, atd.

3.6. Směrování

V komunikačních sítích je možné používat různé způsoby směrování, na jejichž základě směřující uzly (směrovače) doručují datové pakety od zdroje k cíli. Tyto způsoby lze v zásadě rozdělit do následujících skupin:

- **Statické**, u kterých správce sítě ručně zadává směrovací tabulky daného uzlu.
- **Kvazistatické**, které jsou obdobou statických s tím rozdílem, že umožňují definici variantních cest.
- **Distribuované adaptivní metody**, u nichž je směrovací tabulka vytvářena na základě informací, které si uzly samy mezi sebou vyměňují bez zásahu správce sítě.

Pro komunikační síť takového rozsahu, jako je WAN budoucí síť ROWANet, je statické i kvazistatické směrování **nevhodné pro plošné nasazení** z následujících důvodů:

- Náročná údržba směrovacích tabulek a nutnost jejich plošné změny prakticky po jakékoli dílčí úpravě v síti.
- Pomalá nebo žádná reakce na změnu v topologii sítě. Výpadek jedné linky nebo směrovače může vést i k nedostupnosti určité části sítě, přestože do ní existuje cesta.
- Neschopnost využít současně několik ekvivalentních přenosových cest (pokud existují).

Na základě těchto faktů navrhujeme pro WAN síť ROWANet použití **distribuovaných adaptivních směrovacích protokolů**, které jsou v dnešní době implementovány ve všech moderních směrovačích.

Statické směrování je vhodné v síti ROWANET použít pouze například pro výměnu směrovacích informací se sítěmi externích subjektů, kde toto směrování bude mít příznivé vlastnosti především z hlediska bezpečnostních aspektů nebo nad záložní komunikační infrastrukturou ISDN, kde má statické směrování příznivé vlastnosti z hlediska provozních poplatků za telekomunikační služby.

Distribuované adaptivní směrovací protokoly lze dále rozdělit do dvou skupin:

- Protokoly typu **distance-vector**, někdy též nazývané *Bellman-Fordovy*. Směrovače provozující protokoly tohoto typu budují směrovací tabulky na základě výměn topologických informací se sousedními směrovači. Tyto výměny se periodicky opakují a celý proces se ustálí v okamžiku, kdy mají všechny směrovače stejný topologický obraz sítě. Z uvedeného popisu vyplývá, že protokol tohoto typu potřebuje určitý počet iterací k dosažení ustáleného stavu. Počet iterací roste s velikostí sítě. V případě topologické změny v síti je opět potřeba určitý počet iterací k tomu, aby na tuto změnu celá síť správně zareagovala. Popsanému přechodu do ustáleného stavu se říká konvergence. Jako příklad směrovacího protokolu tohoto typu lze jmenovat RIP (Routing Information Protocol) nebo IGRP (Interior Gateway Routing Protocol).
- Protokoly typu **link-state**. Směrovače pracující s těmito protokoly automaticky rozesílají informace o tom, jak vypadá jejich nejbližší okolí. Tyto informace jsou obvykle rozesílány periodicky a navíc vždy v okamžiku, kdy směrovač detekuje ve svém nejbližším okolí nějakou změnu. Toto je základní rozdíl mezi směrovacími protokoly distance-vector a link-state. V případě protokolů link-state si směrovače nevyměňují řádky směrovací tabulky, ale posílají informace o stavu svých vlastních rozhraní a sbírají a přeposílají dále stejné informace získané od sousedních směrovačů. Směrovací tabulka se počítá až následně, na všech směrovacích paralelně. Tento způsob zaručuje podstatně rychlejší konvergenci a vyšší stabilitu celé sítě. Jako příklady směrovacích protokolů tohoto typu lze uvést OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System Protocol), resp. Integrated IS-IS.

Vzhledem k budoucí velikosti komunikační sítě WAN ROWANet je **nejvhodnějším řešením** použití protokolů typu **link-state**. Protokoly typu distance-vector (v IP prostředí tedy RIP nebo IGRP) mohou být použity jako **doplňkové**, například pro některé lokální sítě (LAN) navrhované komunikační sítě. Pro použití protokolů typu link-state hovoří kromě **vyšší stability** a **rychlejší konvergence** také **nižší množství přenášených režijních dat**, což zaručuje efektivní využití přenosových kapacit komunikačních linek.

Výběr konkrétního směrovacího protokolu bude součástí technického projektu.

3.7. Internet

3.7.1. Internetová konektivita

Síť ROWANet lze propojit s veřejnou sítí Internet několika možnými způsoby:

- Získat a provozovat vlastní AS (autonomní systém), získat konektivitu do peeringového centra NIX a dále nakupovat zahraniční konektivitu od dalších ISP (Internet Service Provider). Tento způsob umožňuje zajistit plnou redundanci internetového připojení, tzv. dualhoming.
- Získat vlastní AS a získat připojení prostřednictvím jednoho nebo i více ISP (též plná redundance).
- Nemít vlastní AS a získat připojení prostřednictvím ISP (bez redundance).

Pro připojované subjekty se tedy nabízí možnost připojení k síti Internet:

- prostřednictvím ROWANetu,
- vlastním - prostřednictvím libovolného ISP,
- kombinací předchozích - od ISP, který svou konektivitu transportuje přes infrastrukturu ROWANetu (samostatná VPN).

3.7.2. Distribuce Internetu

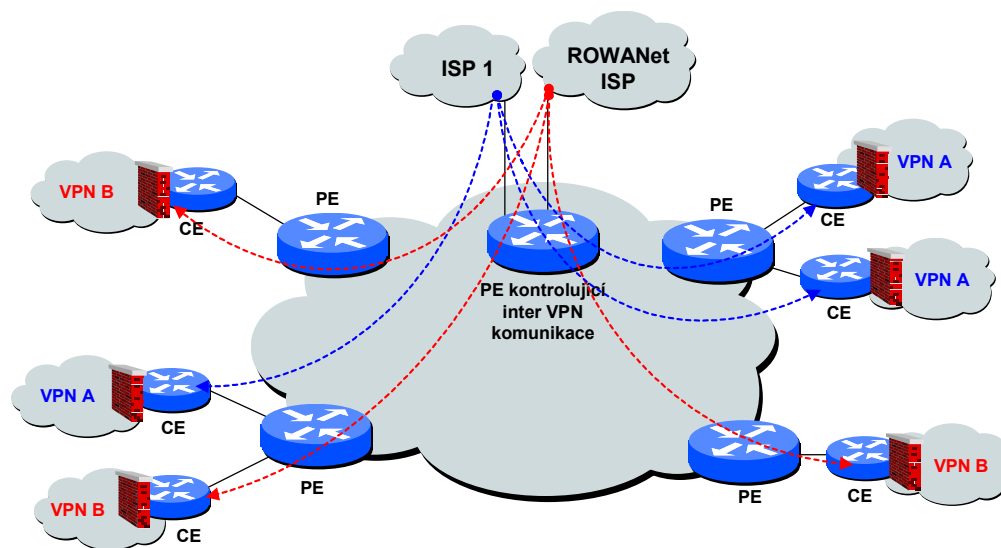
Internet lze distribuovat koncovým subjektům buď ve formě plného (nefiltrovaného) přístupu nebo ve formě přístupu filtrovaného jako službu s přidanou hodnotou. Obě tyto možnosti lze libovolně kombinovat na základě požadavků jednotlivých subjektů.

3.7.2.1. Plný Internet

Nefiltrované (plné) připojení k síti Internet. Filtraci uskutečňuje každý připojený subjekt samostatně. Poskytovatelem připojení může být ROWANet nebo libovolný provider.

Nevýhody: Připojovaný subjekt si musí zajistit vlastní ochranu své lokální sítě (firewall) – finančně náročnější.

Výhody: Připojovaný subjekt má bezpečnostní politiku připojení k Internetu pod svou vlastní kontrolou.



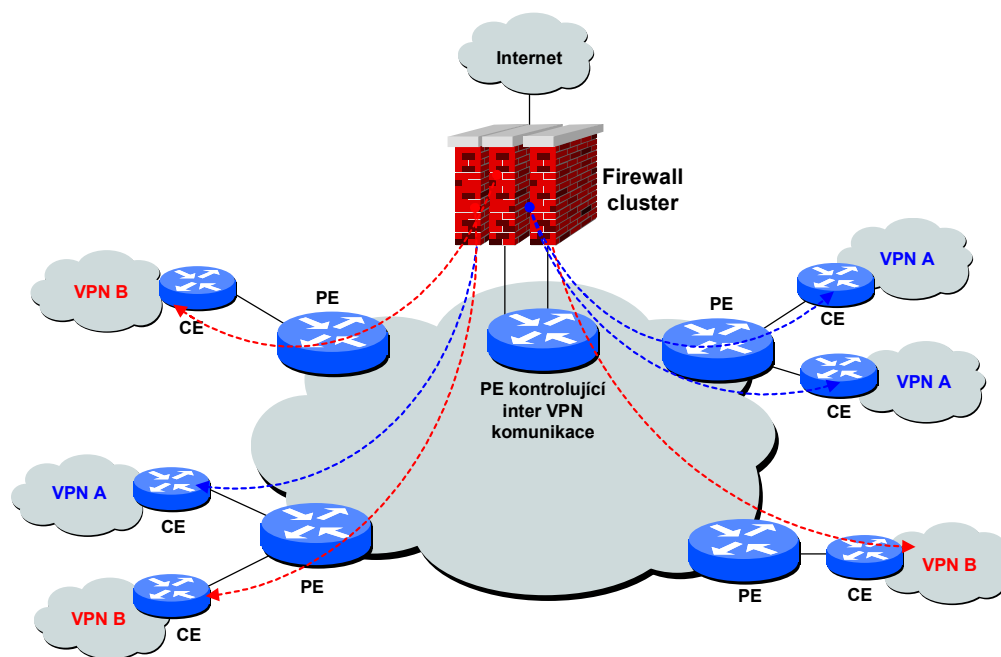
Obrázek 3-18 Plný Internet

3.7.2.2. Filtrovaný Internet

Provozovatel sítě ROWANet může nabídnout službu bezpečného připojení k Internetu svým prostřednictvím. V této variantě provozovatel ROWANetu bude provozovat centrální firewall cluster, jehož prostřednictvím může vybraným subjektům nabízet bezpečné, centrálně filtrované připojení k Internetu.

Výhodou tohoto řešení je, že připojené subjekty nemusí provozovat vlastní firewall z čehož plynou náklady na pořízení a provoz, což může být zejména pro menší subjekty problém. Další výhodou může být centrální bezpečnostní politika.

Nevýhodou se může jevit, že firewall není pod plnou kontrolou připojeného subjektu a zvýšené nároky na administraci firewallu clusteru poskytovatele ROWANetu.



Obrázek 3-19 Centrálně filtrovaný Internet

3.8. Integrace s ostatními sítěmi

3.8.1. GOVBONE

GOVBONE je vyhrazená speciální neveřejná síť (neveřejná virtuální síť) určená pro vzájemnou bezpečnou komunikaci mezi organizacemi veřejné správy a určená ke zprostředkování externí komunikace organizací veřejné správy s jinými subjekty, s veřejností, případně s Internetem a se sítí EU a dalšími subjekty řízeným způsobem.

V současné je k síti GOVBONE připojena většina organizací veřejné správy ČR. Jádrem sítě GOVBONE je tvořeno metropolitní ATM síť FINET-MAN v Praze. Vstupní body do sítě GOVBONE lze také nalézt ve všech okresech ČR. V tomto případě se jedná o VPN vytvořenou prostředky technologie MPLS VPN nad infrastrukturou sítě WAN IS SSP ve správě MPSV.

Pro účely budované sítě ROWANet a k ní připojovaných subjektů lze stávající síť GOVBONE využít pro komunikaci mezi subjekty připojenými k síti ROWANet a organizacemi veřejné správy připojenými k síti GOVBONE resp. pro přístup k službám dostupným na síti GOVBONE.

Přístup ke zdrojům sítě GOVBONE

Přístup subjektu/subjektů připojených k síti ROWANet ke zdrojům sítě GOVBONE lze zajistit bezpečným propojením sítě GOVBONE se sítí ROWANet a to např. připojením sítě ROWANet (přesněji vyhrazené VPN v rámci sítě ROWANet) k nejbližšímu přístupovému bodu sítě GOVBONE (okresní páteří uzel MPLS VPN sítě WAN IS SSP umístěný na ÚP).

Toto propojení lze realizovat:

- běžným propojením na bázi komunikačního protokolu IPv4:
 - výhodou je jednoduchost naznačeného řešení a i nižší cena, protože hraniční směrovače mohou implementovat pouze směrování TCP/IP,
- pomocí technologie Interautonomous MPLS VPN, kdy na rozhraní mezi dvěma uvažovanými sítěmi dochází i k výměně MPLS značek. To lze realizovat samozřejmě pouze za předpokladu, že obě propojované infrastruktury (ROWANet, WAN IS SSP) provozují VPN pomocí technologie MPLS:
 - nevýhoda je v technické náročnosti takového řešení a v potřebě podpory pro funkci Interautonomous MPLS VPN na hraničních směrovačích obou propojovaných sítí.

Variantně lze uvažovat o přímém propojení sítě ROWANet (přesněji vyhrazené VPN v rámci sítě ROWANet) s pražskou metropolitní sítí FINET-MAN.

Přístup jednotlivých subjektů připojených k síti ROWANet k síti GOVBONE a jejím zdrojům je pak možné řídit s využitím prostředků technologie MPLS VPN a samozřejmě je vhodné takové řízení přístupu doplnit o firewallovou ochranu na rozhraní mezi sítí daného subjektu a sítí GOVBONE. Tato firewallová ochrana může být implementována v režii připojovaného subjektu případně může být také nabídnuta jako jedna ze služeb sítě ROWANet.

WAN IS SSP jako komunikační infrastruktura

VPN v rámci WAN IS SSP lze využít i jako na GOVBONE nezávislou komunikační infrastrukturu (samozřejmě za předpokladu dohody s provozovatelem). V takovém případě lze uvažovat např. o využití speciálních propojovacích VPN vytvořených pro účely sítě ROWANet nad MPLS VPN infrastrukturou WAN IS SSP pokrývající dnes prakticky celé území republiky. Ve spolupráci s WAN IS SSP lze tak dosáhnout efektivního propojení libovolných subjektů v rámci ČR. Existují dvě varianty využití této komunikační infrastruktury:

- jednotlivé VPN:
 - pro každý subjekt sítě ROWANet vyžadující transport dat prostřednictvím sítě WAN IS SSP je na této síti vytvořena jedinečná VPN:
 - vhodná varianta zejména v případě nízkého počtu transportovaných VPN.
- hierarchické VPN:
 - s využitím technologie MPLS VPN Carrier supporting Carrier (MPLS VPN CsC) lze dosáhnout transportu všech nebo části MPLS VPN sítí provozovaných v rámci ROWANet s využitím jediné VPN vytvořené pro tento účel na síti WAN IS SSP:
 - vhodná varianta při vysokém počtu transportovaných VPN,
 - nevýhodou je složitá technologie vyžadující kvalifikovaný personál.

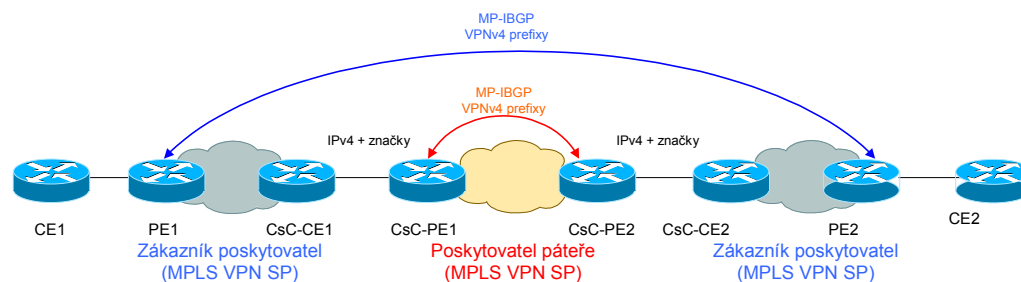
Technologie MPLS VPN CsC umožňuje poskytovateli MPLS VPN služeb (provider páteře) poskytnout svou infrastrukturu jinému MPLS VPN poskytovateli (provider zákazník).

Provider páteře vytvoří pro potřeby providera zákazníka prostředky technologie MPLS VPN (RFC 2574) jedinou VPN, kterou provider zákazník využije pro transport komunikací všech VPN svých zákazníků. Z pohledu providera páteře si lze uvedené řešení představit jako hierarchickou VPN.

Na rozhraní mezi PE směrovačem providera páteře (CsC-PE) a hraničním směrovačem providera zákazníka (CSC-CE¹) je potřeba zajistit výměnu směrovacích informací o PE směrovačích providera zákazníka. Pro tyto účely lze použít protokol BGP-4 (*Border Gateway Protocol*) s implementovanou podporou RFC 3107 (*Carrying Label Information in BGP-4*). Prostřednictvím tohoto protokolu se vyměňují informace o IPv4 adresách PE směrovačů nalézajících se v síti providera zákazníka spolu s příslušnou MPLS značkou.

Následně CSC-CE směrovač redistribuuje obdržené BGP směrovací informace do svého IGP (*Interior Gateway Protocol*) a pro šíření mapování MPLS značek použije protokol LDP (*Label Distribution Protocol*).

Následující obrázek znázorňuje princip výměny směrovacích informací v sítích obou providerů a mezi nimi.



Obrázek 3-20 MPLS VPN CsC - výměna směrovacích informací

3.8.2. Metropolitní síť

O propojení distribučních uzlů ROWANetu a metropolitních sítí částečně pojednává kapitola 3.7.1 ***Chyba! Nenalezen zdroj odkazů.***, ve které je popisováno využití komunikační infrastruktury stávajících metropolitních sítí k distribuci VPN jednotlivých organizací, komunikujících prostřednictvím sítě ROWANet, z distribučních bodů do koncové lokality.

Tato kapitola stručně nastiňuje možnosti (výhody) využití WAN struktury ROWANetu pro jednotlivé subjekty, které jsou připojeny k metropolitním sítím.

Tyto subjekty je třeba rozdělit do dvou základních skupin:

Na **primární subjekty** (např. úřady veřejné samosprávy), se kterými se plánovitě počítá, že budou využívat služeb, které nově budovaná síť bude nabízet a pro něž je síť primárně budovaná a na **sekundární**, tzn. všechny ostatní.

Poznámky:

¹ Z pohledu providera páteře se jedná o CE směrovač.

3.8.2.1. Primární subjekty

Primární subjekty budou moci využívat komunikační infrastruktury sítě ROWANet včetně zdrojů, které plánuje nabízet a ke kterým dané organizace budou mít oprávnění.

Těmto subjektům je též možno prostřednictvím ROWANetu zprostředkovat přístup k síti GOVBONE.

3.8.2.2. Sekundární subjekty

Pro ostatní jednotlivé subjekty je třeba bedlivě zvážit, které služby WAN sítě ROWANet jim bude umožněno využívat.

V úvahu připadá celá škála možností:

- žádná nabídka služeb, tzn. že síť ROWANet bude uzavřenou sítí pro vybrané subjekty,
- zprostředkování připojení k síti Internet,
- zprostředkování připojení k různým zdrojům ROWANetu (veřejné i neveřejné v závislosti na subjektu),
- propojení sítí různých subjektů v rámci distribučních míst ROWANetu,
- v případě oprávněného požadavku, zprostředkování připojení k síti GOVBONE.

4. Dohled a správa síťové infrastruktury, informačních systémů (IS)

Nedílnou součástí budování síťové infrastruktury je vybudování systému pro dohled a správu. Tento systém umožňuje reagovat na chybové stavy jednotlivých prvků, usnadňuje odhalování příčiny poruchy.

Jak se použití IS stává stále samozřejmější součástí běžných činností souvisejících s provozem institucí a firem, narůstá potřeba dostupnosti služeb, které IS nabízí.

Trend, kdy uživatelé vnímají IS jako určitý typ služby (stejně jako dodávky, el. energie, tepla, vody, nebo telefonního spojení) vede k tomu, že uživatelé jsou daleko náročnější jak na dostupnost, tak na kvalitu poskytované služby.

Službami IS pro uživatele můžeme tedy nazývat především ty služby, které jsou schopni uživatelé identifikovat. Jedná se tedy např. o služby přístupu do sítě Internet, přístup k jednotlivým web serverům, možnost přijímat a odesílat elektronickou poštu, možnost poslouchat rozhlasové zpravodajství přes internet, fungující aplikace pro činnost uživatele (ekonomický SW, nástroje pro projektování, textové editory, ...).

Z tohoto důvodu se i systémy pro dohled IS přestávají zaměřovat na dohled a správu jednotlivých prvků a zařízení jako doposud, a soustředí se na dohled služeb a jejich kvalitu.

Dohledové prostředky musí umožňovat nepřetržité sledování kritických systémů a umožňovat rychle reagovat na chybové stavy.

Důležitou součástí nasazení systému, který umožní dohled a správu je vybudování odpovídajícího pracoviště, které bude řešit problémy a předcházet chybovým stavům.

4.1. Modely správy IS

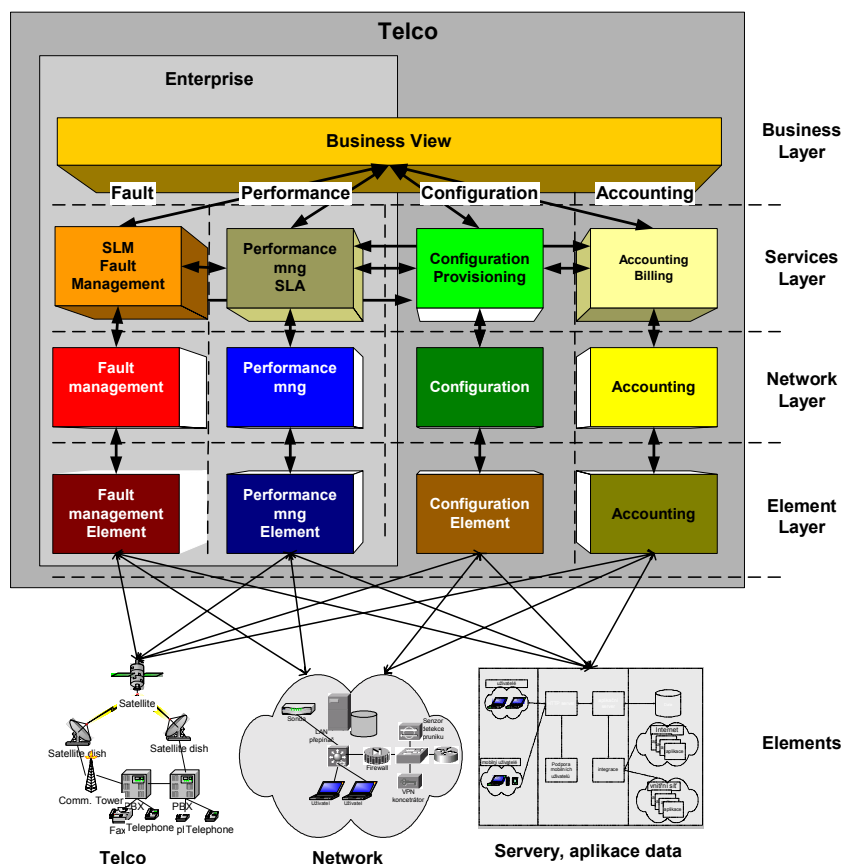
Pro dohled a správu IS bylo definováno několik modelů, které specifikují způsob a oblasti pro dohled. Základní model je tzv. ISO model. Tento model ovšem v současnosti neodpovídá požadavkům na moderní dohled IS a je nahrazován tzv. Telco modelem.

4.1.1. ISO modelu

Správa informačních systémů dle definice ISO standardů; se člení na tyto oblasti:

- Fault management - sledování chybových stavů
- Performance management – sledování výkonu
- Configuration management – správa konfigurací
- Accounting - účtování
- Security management – správa zabezpečení

4.1.2. Telco model



Tento model dělí aplikace pro dohled do vertikální a horizontálního rozdělení. Horizontální rozdělení je podle typu získávaných a prezentovaných informací.

Tento model je převážně využíván pro poskytovatele služeb (telekomunikační společnosti), které potřebují nejen sledovat zařízení, ale poskytují zákazníkům informace o stavu poskytovaných služeb.

Z hlediska oblastí dohledu se jedná o 4 základní oblasti:

- Fault management - sledování chybových stavů
- Performance management – sledování výkonu
- Configuration management – správa konfigurací
- Accounting – účtování

Tyto oblasti jsou rozděleny podle míry integrace a pohledu na IS na elementární dohledové systémy, síťové systémy a systémy pro dohled služeb. Nad dohlíženými službami poskytují provozovatelé informační systémy, které jsou schopny poskytovat informace o kvalitách služeb. Celý systém je otevřen i pro možné propojení s tzv. obchodními procesy společnosti, které jsou závislé na IS.

4.1.3. FAB model

Velmi populární je použití tzv. FAB modelu, který přistupuje ke způsobu dohledu IS z hlediska dohlížení služeb.



Model je členěn na tři základní funkční celky – vytváření a údržba služeb, zajištění kvality a dostupnosti služeb a účtování/zákaznická péče.

Z hlediska dohledu kvality služeb je nejdůležitější oblastí tzv. Service Assurance – zajištění služeb. Tato oblast je řešena systémy pro sledování chybových stavů a systémy pro sledování výkonnosti (fault a performance management). V dalším textu se budeme zabývat právě těmito oblastmi.

4.2. Systémy pro zajištění služeb – Service Assurance

4.2.1. Systém sledování dostupnosti a provozu v síti - performance management

Dostupnost prvků IT se zpravidla definuje ve vztahu k uživatelům a bezpečnosti. Bezpečnostní politika definuje “kdo s kým”, tj. pravidla, kteří uživatelé mají mít přístup ke kterým zdrojům IT. Přesněji, kdy jednotlivé skupiny uživatelů mají bezpečnostní politikou definována přístupová práva k přesně vymezeným zdrojům (serverům, databázím, aplikacím apod.). Dostupností se myslí, že tyto zdroje jsou jim k dispozici vždy, když je potřebují. Ve větších komunitách uživatelů s rozprostřenou pracovní (nepřetržitou) dobou to znamená, že systém řízení sítě musí zajistit nepřetržitou provozuschopnost IP sítě. Provozuschopnost kromě robustnosti (odolnosti vůči poruchám linek, výpadkům jednotlivých směrovačů či jejich interface) a IP konektivity znamená, že všechny prvky (např. přenosové linky, vyrovnávací paměti ve směrovačích atd.) mají dostatečnou dynamickou kapacitu v průchodnosti.

Průchodnost lze teoreticky odhadnout a modelovat simulačními experimenty. Podle výsledků modelování pak odpovídajícím způsobem dimenzovat prvky IP sítě. V laboratorních a pilotních zkouškách lze teoretický návrh ověřit. V průběhu zkušebního provozu je třeba sledovat vybrané prvky IT (tak, aby bylo možné statisticky vyhodnotit jejich provozní zátěž).

To je umožněno mechanismem opakovaných dotazů (device polling), kterými systém řízení a dohledu sbírá informace ze sledovaných zařízení (protokolem SNMP podle MIB) a ukládá je do databáze. Následné vyhodnocení těchto údajů poskytne informace o vytížení jednotlivých (kritických) prvků IT.

Z funkčního hlediska je důležitý pečlivý výběr sledovaných charakteristik tak, aby byly relevantní. Druhé hledisko je technické, protože sběr dat po delší dobu je náročný na diskovou paměť.

Cílem funkční specifikace je stanovení požadované robustnosti a kritérií dostupnosti, potažmo sledovaných charakteristik. Cílem celkového řešení je pak volba vhodného modelu řídicího systému a jeho návrh a realizace, s následným systémem sledování dostupnosti.

Pro sledování provozu v síti nebo přímo pro pořízení údajů umožňujících účtování v závislosti na využití přenosové kapacity sítě jednotlivými uživateli nebo skupinami uživatelů, je nutné získat přesné údaje o využívání síťových zdrojů a definovat systém další správy těchto dat, resp. způsob získávání účtovacích dat ze síťových prvků, resp. aplikací, sumarizaci pořízených údajů a jejich úschovu. K dosažení tohoto cíle je možné využít několika prostředků, přičemž vhodnost každého z nich přímo závisí na tom, pro jaký účel jsou tato data sbírána. Mezi základní zdroje účtovacích dat patří:

- účtovací služby Cisco IOS,
- systém RMON,
- systém řízení sítě.

Sběr dat přímo v systému řízení sítě je nástroj umožňující sledovat zatížení jednotlivých linek nebo segmentů sítě. Tento prostředek je vhodný pro sledování propustnosti sítě a odstraňování úzkých míst systému. Využití těchto dat v systému účtování je však poněkud problematické z důvodů problematického určení zdrojů, resp. cílů dat.

Cílem funkční specifikace systému účtování je definovat účtovací funkce, typy sbíraných dat a požadované výstupy tohoto systému. V technické specifikaci se pak vybere vhodná kombinace výše popsaných metod sběru a vyhodnocování dat.

4.3. Systém správy chybových stavů sítě – fault management

Správa chybových stavů neboli fault management je základní a nezbytnou součástí komplexního managementu sítě, protože právě poruchy v síti, na níž je odkázán provozovatel, jsou samozřejmě nejčastějším důvodem výpadků informačních systémů a mohou znamenat významnou finanční ztrátu a nespokojenost uživatelů. Tato oblast zahrnuje funkce identifikace, separování a napravení poruch a problémů v činnosti sítě (její integrální částí je podávání výstražných zpráv, které mají za úkol informovat uživatele o poruchách sítě nebo jejích součástí a o abnormální činnosti). Management v případě poruch musí mít přístup ke všem síťovým zdrojům, vzdáleným i místním, aby bylo možné detekovat poruchy a dálkově aktivovat diagnostické testovací programy. Dále musí dovolit síťovému operátorovi iniciovat zprávy týkající se údržby, které mohou být posílány všem uživatelům sítě, dokázat srovnat poruchy podle důležitosti a okamžitě uvědomit operátora o významných nových poruchách, periodicky informovat o významných dlouhodobých poruchách tak, aby výpadek řídicího systému neměl dopad na běžný provoz v síti.

Správa chybových stavů a poruch by měla zahrnovat všechny oblasti správy komplexní síťové infrastruktury a především by se v ní měly objevit chyby a poruchy z těchto sledovaných oblastí:

- management síťových zařízení,
- systém pro sledování služeb,
- sledování serverů,
- management produktů pro zabezpečení IS.

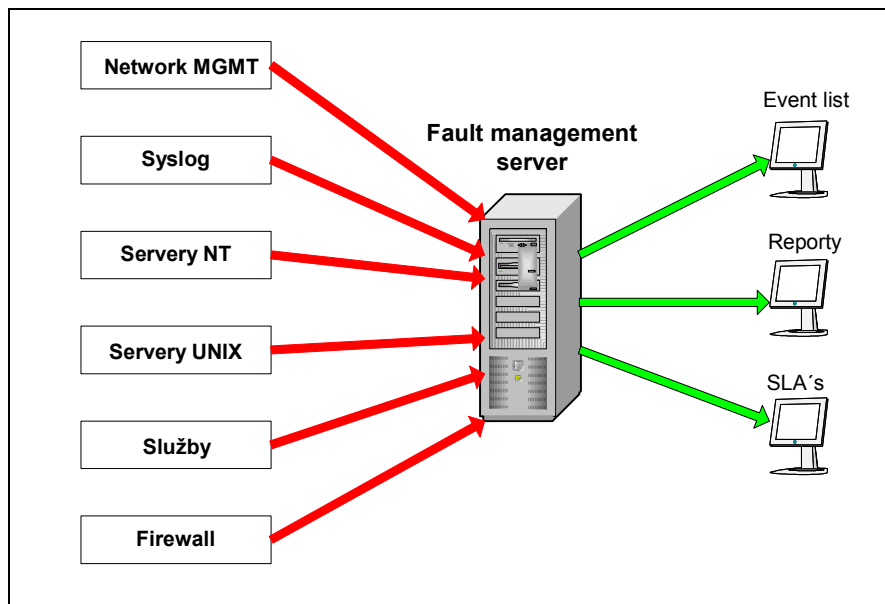
V ideálním případě je žádoucí, aby se všechny informace získané z komunikační infrastruktury přenášely do jednotné management platformy. Tento krok zjednodušuje následnou správu a umožňuje administrátorům flexibilně reagovat na chybové stavy a poruchy, které nastanou v dané infrastruktuře.

Tuto podmínku je v současné situaci, kdy existuje pro správu komplexní síťové infrastruktury množství specifických nástrojů, těžké splnit. Proto je nutné se snažit tyto oddělené prvky integrovat a zastřešit pod jednotný management nástroj, který bude schopen z těchto specifických nástrojů čerpat cenné informace, zpracovat je a prezentovat směrem k uživateli (administrátorovi) v čitelné a přehledné formě.

Komplexní fault management by měl splňovat resp. nabízet následující funkce:

- správa a integrace alarmů a eventů z mnoha nezávislých zdrojů do jednotného rozhraní, což zabezpečí i zjednodušení práce management operátorů,
- konsolidaci událostí, de-duplikace, filtrování a redukce množství informací, které dostává operátor,
- distribuovaná architektura, která nabízí možnost přístupu ze vzdálených lokalit, Java resp. Web-based podpora,
- zpracování informací v reálném čase - automatické zpracování událostí, které se provádí na základě definovaných pravidel. Jedná se o obecná pravidla a o uživatelsky definované akce a nastavení. Tyto akce jsou definovány na základě chování IS,
- Fail-over – tj. podpora proti výpadku aplikace. Jedná se o podporu hot standby konfigurace pro automatické přesměrování zpracování na záložní stanici, nebo podpora store-and-forward režimu pro uchování dat,
- definice automatických akcí a reakcí na příchozí události,
- korelace událostí,
- možnosti vyrozumění management operátorů, při výskytu např. Kritických událostí – např. mail, pop-up alert, pager, trouble ticket, log soubory,
- podpora sběru událostí a chybových stavů v heterogenním prostředí tj. přepínače, směrovače, huby, servery (windows, unix), služby, bezpečnostní zařízení (firewall) atd.,
- možnost integrace na reportovací mechanismy, Service Level Agreement nástroje atd.,
- jednoduchá instalace, konfigurace a správa.

Následující obrázek ukazuje schéma komplexního fault managementu z pohledu sledovaných elementů. Zabezpečit sledování chybových stavů a událostí je prvotním úkolem managementu. Tento úkol by měl zastřešit pod jednotným rozhraním. Na druhé straně jsou znázorněny výstupy, které by měl být schopen poskytovat na základě získaných údajů.



Obrázek 4-1 Funkčnost komplexního fault managementu

4.4. Sledování služeb

4.4.1. Služby v IP síti

Co rozumíme pod pojmem služba IP sítě

Moderní IP síť musí kromě základní služby IP konektivity poskytovat i další infrastrukturu, která je nutná pro chod běžných síťových aplikací.

Za základ tvořící tuto infrastrukturu lze považovat následující služby:

- IP konektivita,
- DHCP,
- DNS,
- WINS,
- NTP.
- FTP,
- WWW,
- elektronická pošta,
- atp.

Z hlediska sledování lze pojem služby zobecnit a za službu považovat například i napájení jednotlivých síťových prvků, vytížení CPU WWW serveru atd.

Služby lze rozdělit na 2 skupiny:

- služby elementární,
- služby složené.

Služby složené vzniknou spojením několika služeb elementárních nebo složených. Lze tak vytvořit i vícestupňovou hierarchickou závislost mezi různými službami. Podrobné dělení a hierarchická struktura služeb usnadňuje především diagnostiku chybových stavů.

Příkladem složené služby je služba elektronické pošty, která závisí na jednodušších službách. Například na:

- IP konektivité uživatele a serveru, kde je uložena poštovní schránka,
- IP konektivita serveru se schránkou a Internetu,
- jmenných službách DNS,
- množství prostoru na disku serveru se schránkou.

4.4.2. Kvalita služeb

U všech služeb lze sledovat různé ukazatele, například:

- dostupnost – existence,
- doba odezvy,
- propustnost (vytížení).

Primárním měřítkem kvality služby je její dostupnost. Informace o kvalitě služby by měla zahrnovat jak okamžité hodnoty sledovaných parametrů, tak jejich historickou analýzu.

Lze rozlišit 2 pohledy na služby sítě, pohled uživatele (zákazníka) a pohled administrátora (poskytovatele služby), které je třeba respektovat při prezentaci výsledků sledování.

Uživatel posuzuje funkčnost sítě podle funkčnosti své síťové aplikace (například podle funkčnosti svého programu pro přístup k elektronické poště) a nezajímá se o podrobnosti implementace. Uživatel sleduje pouze nejvyšší úroveň hierarchie služeb.

Administrátor naopak sleduje všechny úrovně služeb, aby mohl udržovat vysokou kvalitu služeb, předcházet zhoršování kvality a rychle analyzovat vzniklé problémy.

V diskusích o řešení vztahu zákazník - poskytovatel se čím dál častěji setkáváme s pojmy Service-Level Management (SLM, Správa úrovně služeb) a Service-Level Agreement (SLA, Dohoda o úrovni služeb).

Správa úrovně služeb (Service-Level Management)

Od roku 1997 lze v oblasti správy velkých informačních systémů (IS) sledovat odklon od tradičních forem správy oddělených komponent IS k nové generaci nástrojů pro správu. Objektem správy přestaly být jednotlivé komponenty IS, ale staly se jím komplexní služby, poskytované uživatelům jako zákazníkům.

Nástroje pro správu úrovně služeb shromažďují údaje ze sledování celého IS, konsolidují je a poskytují přesný, jednoznačný a uživatelsky definovatelný pohled na stav kritických aplikací a služeb v reálném čase. Pohled na stav IS se prezentuje mnoha různým skupinám uživatelů - administrátorům, operátorům, obyčejným uživatelům zákazníka i vrcholnému managementu. Nástroj musí být schopen přizpůsobit zobrazované informace všem úrovním znalostí a oprávnění.

Kromě zobrazení stavu služeb v reálném čase musí nástroj zpracovávat i přehledy o stavu služeb za určité období a reagovat na snižování úrovně služby v dané časové periodě, podle předem specifikovaných procedur.

Údaje, které nástroj pro SLM poskytuje, slouží jako základ pro tvorbu a kontrolu "smluv o úrovni služby" (SLA, Service-Level Agreement).

Smlouva o úrovni služby (Service Level Agreement)

Důležitým nástrojem diferenciací mezi různými poskytovateli služeb IS je schopnost garantovat nabízené služby. Definice nabízených služeb, jejich garantovaných ukazatelů a způsob jejich kontroly ze strany zákazníka jsou obsahem "smlouvy o úrovni služby" (SLA). Na základě přijaté smlouvy o úrovni služby může zákazník i poskytovatel pomocí nástrojů pro SLM sledovat plnění podmínek SLA.

Role zákazníka a poskytovatele lze definovat nejen mezi dvěma různými organizacemi, ale i v rámci jedné organizace mezi oddělením spravujícím IS a ostatními odděleními, které využívají infrastrukturu IS.

4.4.3. Systém sledování služeb

Systém sledování kvality služeb by měl umožnit definovat poskytované služby, s uživateli dohodnout požadovanou dostupnost (availability) služeb, určit podpůrné elementy těchto služeb a následně kontrolovat dodržování dohod. Mezi tyto služby patří, např. zaručení max. výpadku tiskárny oddělení po dobu jedné hodiny. To znamená, že servisní oddělení se zaváže do jedné hodiny po ohlášení poruchy tiskárny buď ji uvést opět do chodu, anebo ji vyměnit za jinou - funkční. Systém sleduje stav poruchy (ohlášená, započato s opravou, příčina zjištěna, skončena) a dobu opravy. Stejnou informaci mohou získat uživatelé, kteří jsou chybovým stavem postiženi. Systém může rovněž sledovat dobu opravy a při jejím překročení může automaticky problém hlásit vyšší řídicí úrovni nebo eskalovat problém středisku podpory výrobce či dodavatele zařízení.

Jiná dohoda o kvalitě služeb se může týkat rychlosti přístupu z pracovních stanic na povolené servery (zaručená doba odezvy apod.).

Jasně specifikované vlastnosti a úroveň služeb rovněž usnadní komunikaci s uživateli.

Je jasné, že náklady na servisní činnost rostou s kvalitou služeb. Je proto vhodným kompromisem mezi náklady a úrovní služeb. Systém sledování služeb rovněž může automaticky sumarizovat náklady za služby poskytované různými odděleními uvnitř organizace.

4.4.3.1. Jak sledovat kvalitu služeb obecně

Služby lze sledovat různými způsoby, které se liší implementací, náročností administrace i vypovídací hodnotou.

- sledování IP konektivity a funkčnosti hlavních komponent služby - nejjednodušší způsob s nejnižší vypovídací hodnotou a implementační náročností. Příkladem je sledování funkčnosti WWW serveru pomocí SNMP agenta, který podává informaci o běžících službách v operačním systému MS Windows NT.
- funkční sledování z centrální řídicí stanice - na řídicí stanici běží agenti, kteří cyklicky testují funkčnost služby. Příkladem je agent, který stahuje definovanou HTML stránku z daného WWW serveru. Tento způsob plně ověřuje funkčnost WWW serveru pro definovanou HTML stránku, nepokrývá však prostorové rozložení dostupnosti služby z různých míst sítě. Implementačně je náročnější, vyžaduje zvláštního agenta pro každý typ služby.
- funkční sledování pomocí distribuovaných agentů - nejvěrněji zobrazuje stav služby i z prostorového hlediska. Agenti ověřující službu jsou umístěni do vybraných míst sítě. Je administrativně nejnáročnější. Vyžaduje umístění vhodného operačního systému do vybraných míst sítě a zajištění přenosu zjištěných dat na centrální řídicí stanici, která je vyhodnocuje.

Nedílnou součástí sledování služeb je vyhodnocování zjištěných údajů a distribuce informace o kvalitě služeb. Jako nejvhodnější se jeví následující způsoby zpracování výsledků sledování.

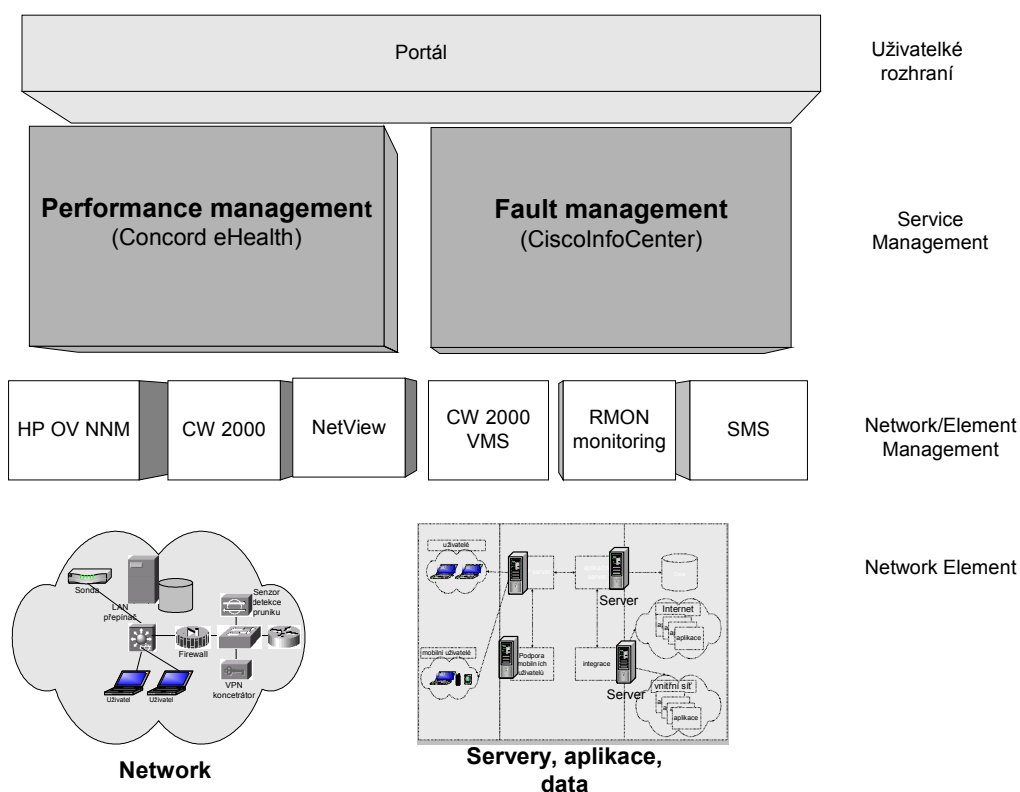
- HTML stránky - nejvhodnější způsob pro informování běžných uživatelů.
- Telnet přístup a zobrazení informací pomocí příkazu z příkazové řádky - způsob vhodný pro nouzový vzdálený přístup administrátorů.
- rozhraní do HelpDesku - vyžaduje alespoň částečnou filtraci přenášených událostí, aby se zamezilo zahlcení HelpDesku falešnými nebo opakujícími se poplachu. Přínosem je využití procedur pro vyhodnocení problémů, které existují v HelpDesku a sledování jejich řešení.
- přímé vyrozumění odpovědných osob - vyžaduje provést vyhodnocení vzniklých událostí a alespoň základní verifikaci vyrozumění přímo na řídicí stanici. Lze využít běžných způsobů předávání zpráv (e-mail, SMS, paging).

4.5. Řešení dohledu IS

Řešení dohledu IS souvisí s požadavky, které na systém máme. Pro základní dohled je nutné vybudovat systémy, které jsou schopny získávat informace z jednotlivých prvků. Jedná se o vybudování základního tzv. elementárního dohledového systému. Tyto systémy jsou převážně určeny pro operátory a administrátory jednotlivých systémů (serverů, síťových zařízení, operačních systémů, atd.).

Pro potřeby komplexního pohledu na stav služeb IS, je nutné nasazení systémů, které jsou schopny integrovat informace z různých systémů a sledovat služby.

Pro poskytovatele služeb a velké organizace je potřeba zpřístupnění informací prostřednictvím portálového řešení. V tomto případě uživatelé jsou informováni o stavu IS.



4.5.1. Nasazení elementárních systémů dohledu

Dohled IP zařízení

Pro základní dohled IP sítě doporučuje využít aplikaci, která zobrazí IP zařízení a umožní základní správu síťových prvků:

- Zobrazení prvků v mapě,
- Dotazy na zařízení zda jsou dostupné včetně barevné interpretace nedostupnosti
- Zpracování chybových stavů – SNMP trapů
- Sběr dat

Jako elementární dohledový systém můžeme použít např. aplikace typu HP OV NNM, SNMPc, WhatsUp Gold.

Sledování chybových stavů – fault management

Pro sledování chybových stavů, které jsou jednotlivými prvky IP sítě charakterizovány generováním SNMP trapů, je možné pomocí aplikací pro dohled IP zařízení (HP OV NNM, SNMPc).

Tyto aplikace umožňují sběr chybových stavů, jejich třídění, generování automatických akcí na jednotlivé chybové události.

Sledování provozu – performance management

Pro sledování provozu, vytížení linek je možné využít nástroje, které jsou schopny sbírat statistiky pomocí SNMP protokolu. Jedná se např. o freeware aplikace MRTG. Tato aplikace umožňuje sledování statistik.

Možnost sledování těchto charakteristik je možné i pomocí aplikací HP OV NNM a SNMPc.

Informace jsou dostupné přes web rozhraní.

4.5.2. Nasazení systémů pro dohled služeb a integraci informací

Systémy pro dohled služeb a integraci informací sbírají informace jak z jednotlivých prvků, tak dokáží využívat informace z jednotlivých aplikací které vykonávají elementární dohled prvků.

Stejně jako v předchozím případě je z hlediska dohledu služeb důležité zaměření na dostupnost služby, její chyby, a na kvalitu služby.

Fault management

Sledování chybových stavů včetně poklesu kvality je řešeno systémy pro fault management, které dokáží korelovat informace z různých zdrojů.

Jedná se např. o systém Micromuse Netcool, který umožňuje sběr dat ze všech systémů a následnou korelaci, vyhodnocení problémů. Systém je možné doplnit rozhraním pro uživatele služby a v případě kdy je poskytovatel služby potřebujeme dokumentovat stav jednotlivých služeb, je tento systém schopen poskytovat tyto informace přehledným uživatelským portálem.

Performance management

Z hlediska sledování kvality služeb je nutné sledovat množství informací v rámci IS a tyto informace vzájemně provázat.

Řešením sledování kvality služeb IS je např. aplikace Concord eHealth, která dokáže sbírat informace pomocí SNMP protokolu, netflow, a zároveň umožňuje import dat z nezávislých datových zdrojů. Aplikace umožňuje nastavení uživatelských reportů, které zobrazují kvalitu komponent a služeb poskytovaných uživatelům. Stejně jako v předchozím případě jsou data dostupná přes uživatelský portál a je možné je prezentovat „zákazníkům“, uživatelům používající služby.

4.6. Způsoby provozování systémů pro dohled IS

Provozování systémů pro dohled IS je nutné zabezpečit nejenom technicky, ale i organizačně a hlavně mít dostatečné lidské zdroje – odborníky, kteří budou schopni s nástroji pracovat, vyhodnocovat informace a řešit problémy.

Zabezpečení nasazení systémů je možné realizovat několika způsoby. Možná řešení jsou např. následující:

- Systém pro dohled IS včetně zabezpečení lidských zdrojů.
- Systém pro dohled IS, zabezpečení lidských zdrojů externí organizací.
- Dohledu a správa IS externí organizací (outsourcing).

4.6.1. Nasazení systémů pro dohled IS a zabezpečení lidských zdrojů

Toto řešení vyžaduje zpracování kvalitního projektu a koncepce dohledu IS. Součástí systému musí být samozřejmě zabezpečení rozvoje a údržby takového systému (možnost dohledu nových technologií, údržba stavu aplikací a op. Systémů).

Dále je nutné zabezpečit příslušné lidské zdroje – odborníky pro jednotlivé technologie a techniky, kteří budou schopni reagovat na výskyt problémů a chybových stavů v IS. Je nutné počítat s potřebou odborného rozvoje těchto pracovníků.

Výhodou tohoto řešení je maximální možnost získání informací o stavu IS, komunikace mezi uživateli a administrátory.

4.6.2. Nasazení systémů a zabezpečení lidských zdrojů externí organizací

Toto řešení stejně jako předchozí vyžaduje zpracování kvalitního projektu a koncepce dohledu IS. Součástí systému musí být samozřejmě zabezpečení rozvoje a údržby takového systému (možnost dohledu nových technologií, údržba stavu aplikací a op. Systémů).

Oproti předcházejícímu řešení nemusíme řešit problémy s lidskými zdroji.

V tomto případě je nutné mezi servisní organizací a zákazníkem specifikovat vstupy a výstupy, způsoby zabezpečení informací, předávání si zpráv o chybových stavech.

Tento způsob z hlediska zákazníka umožňuje v případě nedodržení požadované kvality dohledu IS změnit společnost, zabezpečující lidské zdroje s tím, že implementované systémy v plné míře umožní dohled a správu IS zákazníka a je možné využít jiného dodavatele, který nad těmito prostředky bude dodávat spolehlivější podporu a služby.

Nevýhodou systému jsou investice do systému a také možná menší informovanost o stavu IS, nutnost precizního nastavení komunikace mezi externí organizací a uživatelem.

4.6.3. Vyřešení dohledu a správy IS externí organizací (outsourcing)

Jedná se o provozování služby formou outsourcingu.

Systémy jsou instalovány u externí organizace. Ta zabezpečuje jak dohled a správu IS, tak potřebné lidské zdroje pro zabezpečení dané služby.

V tomto případě je nutné mezi servisní organizací a zákazníkem specifikovat vstupy a výstupy, způsoby zabezpečení informací, předávání si zpráv o chybových stavech.

Tento způsob je z hlediska zákazníka nejjednodušší, nejsou zde žádné nároky na údržbu a rozvoj dohledových systémů, na lidské zdroje a s tím související investice (plat, školení, podpora).

Nevýhodou systému může být menší informovanost o stavu IS, nutnost precizního nastavení komunikace mezi externí organizací a uživatelem.

5. Služby vyšších vrstev

5.1. Společné zásady budování vyšších služeb OSI modelu

Budování služeb vyšších vrstev OSI modelu odpovídá postupům ověřeným v mnoha jiných projektech. Služby sítě jsou nadstavbou nad IP konektivitou poskytovanou komunikační infrastrukturou ROWANetu. Služby sítě lze budovat postupně nad komunikační infrastrukturou, vždy s ohledem na dostupné finanční prostředky a potřeby uživatelů ROWANetu.

Řešení musí respektovat současné požadavky investora, ale zároveň umožnit jeho další rozvoj při zachování doposud vynaložených investic. Navržené řešení být škálovatelné, tj. musí umožnit přidávat další prvky do systému bez nutnosti složité rekonfigurace všech stávajících prvků. Řešení musí umožnit použití kombinace produktů několika různých výrobců. Návrh sítě ROWANet by měl respektovat zásady, na kterých je vybudován Internet (původní ARPANET), tj. distribuovaný systém s minimem kritických bodů selhání (single point of failure).

Řešení musí respektovat mezinárodně uznávané zásady, musí být postaveno na otevřených standardech, především na příslušných doporučeních RFC (Requests for Comments). ROWANet musí vyhovovat pravidlům stanoveným pro budování KIISVS a dalším českým a evropským zákonům a normám.

ROWANet jako distribuované řešení ale zároveň nesmí bránit sdružování zdrojů, kapacit a prostředků tam, kde je to výhodné nebo kde se na tom jednotlivé připojené subjekty spolu dohodnou.

Prostředí ROWANetu musí umožnit provozovat připojeným subjektům své informační systémy v různých režimech: od provozování vnitřního IS vlastními silami až po úplný outsourcing všech částí VIS. V praxi se zřejmě nejčastěji bude vyskytovat smíšený mód, kdy část IS si bude provozovat a spravovat připojený subjekt sám, a pro část bude využívat různé formy outsourcingu.

Lze si představit, že několik spřátelených obcí zakoupí dohromady jeden server a na něm bude provozovat své vlastní informační systémy s jedním společným správcem, nebo si služby nakoupí u některého z místních komerčních subjektů připojených do ROWANetu.

Při respektování standardů pak bude možno realizovat služby ROWANetu na směsici hardwarového i softwarového vybavení. Kde to bude výhodné, lze využít komerčních řešení, jinde zase (například z licenčních důvodů) bude vhodné zvolit řešení vybudované na Open Source.

5.2. Bezpečnost sítě ROWANet

V síti ROWANet bude postupně nasazena celá řada bezpečnostních prvků, tak aby v každém okamžiku nabízela nejlepší poměr cena/výkon. Tyto prvky budou zajišťovat vyšší úroveň bezpečnosti než je obvyklé u poskytovatelů Internetu (Internet Service Provider – ISP). Budou nabízet uživatelům širokou škálu bezpečnostních prvků a služeb, které uživatelé ROWANetu budou moci dle svého uvážení využívat. Některé z bezpečnostních prvků budou primárně sloužit provozovateli sítě ROWANet, tak aby mohl zajistit požadovanou kvalitu služeb. Bezpečnostní prvky mohou být také využity při dohledu sítě.

Navrhované řešení musí být připraveno na budoucí zvyšující se nároky, na zvýšení provozu, na možné změny zákonného prostředí. Důležité je, že bezpečnostní systém je možno budovat postupně, tak, jak se budou vyvíjet potřeby uživatelů ROWANetu.

5.2.1. Základní teze

Celé řešení otázek bezpečnosti uvnitř sítě ROWANet je založeno na několika základních principech, se kterými musí souhlasit všichni uživatelé:

Každý subjekt je plně odpovědný za svoji vlastní bezpečnost

Odpovědnost za bezpečnost svých systémů má každý připojený subjekt. Za svou bezpečnost si odpovídá každý sám. K zajištění bezpečnosti může využít vlastních zdrojů, může část bezpečnosti outsourcovat, může využít služeb, které nabízí centrální bezpečnostní prvky ROWANetu.

Bezpečnost není stav ale nikdy nekončící proces

Žádný systém není úplně bezpečný, bezpečnost systému je omezena jeho nejslabším článkem. 100% bezpečný systém neexistuje. Bezpečnost nelze zajistit tím, že jednorázově nakoupíme nejdražší bezpečnostní prvky, správně je nastavíme a můžeme se o bezpečnost přestat starat. Znalostí hackerů se každý den mění, mění se i způsoby obrany proti útokům. Tomu musí odpovídat i chování připojených subjektů.

Každý subjekt si sám určuje své partnery pro komunikaci

Značná část škodlivého kódu se šíří nevyžádanou poštou a přístupem na „nebezpečné“ stránky. Existují technologie, které umožní administrátorům připojeného subjektu nastavit pravidla pro komunikaci tak, aby odpovídala bezpečnostní politice připojené organizace, aby respektovala dohody, které má připojená organizace uzavřeny s dalšími připojenými subjekty.

Využívání centrálních bezpečnostních prvků ROWANetu je dobrovolné

Pokud si to připojený subjekt bude přát, může ROWANet sloužit pouze jako poskytovatel IP konektivity do Internetu, veškeré centrální bezpečnostní prvky budou pro připojení tohoto subjektu ignorovány. Na druhou stranu, provozovatel ROWANetu musí mít právo chránit ostatní připojené subjekty před eventuální škodlivou činností tohoto subjektu.

Nejslabším článkem řetězu jsou lidé

Jak vyplývá z mnoha bezpečnostních rozborů a statistik, nejslabším článkem bývají lidé. Proto je potřeba věnovat velkou pozornost neustálému vzdělávání všech osob, které využívají možnosti připojení k ROWANetu.

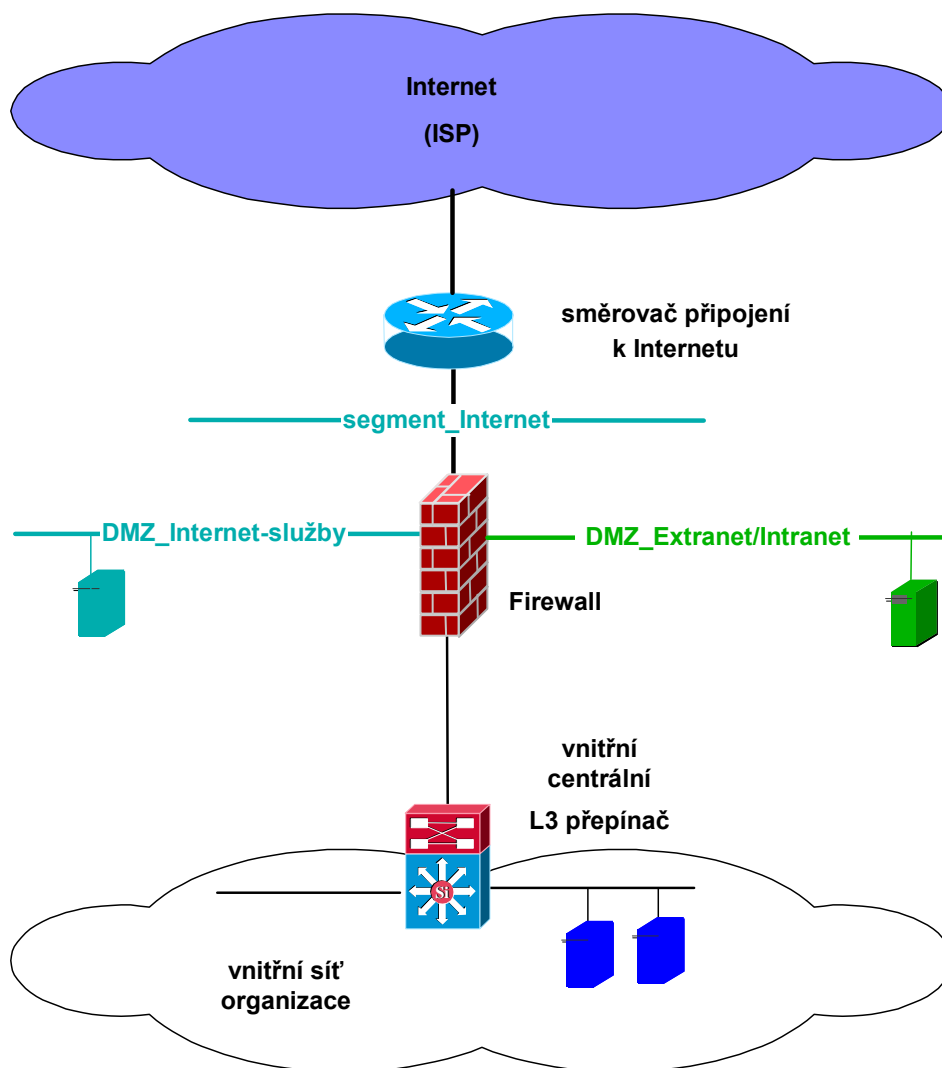
5.2.2. Bezpečnostní prvky

Veškeré nastavení bezpečnostních prvků by mělo odpovídat bezpečnostní politice ROWANetu i bezpečnostním politikám připojených subjektů.

5.2.2.1. Firewall

Firewall (FW) je základní bezpečnostní prvek. Slouží k oddělení vnitřní sítě připojeného subjektu od okolních, potenciálně nebezpečných sítí. Každý připojený subjekt by svoji LAN měl chránit firewallem. V závislosti na použitém řešení lze na firewallu nastavit pravidla pro komunikaci tak, jak to odpovídá bezpečnostním požadavkům připojeného subjektu.

Firewall nemusí sloužit jen jako ochrana před vnějším nebezpečím, při správném návrhu a konfiguraci lze firewall použít i k ochraně citlivých dat proti útokům (zcizení, změna, ...) zevnitř organizace. Je více způsobů, jak toho docílit, jedním ze způsobů může být firewallová soustava nebo firewall s několika demilitarizovanými zónami (DMZ). Jeden z příkladů je uveden na následujícím obrázku.



Obrázek 5-1 Bezpečné připojení organizace k Internetu

Řešení firewallu je možno různými způsoby outsourcovat – od pronájmu hardwarového zařízení a smlouvy o jeho správě s externím subjektem, až po zakončení připojené VPN na centrálních firewallech a dohodou s provozovatelem ROWANetu o správě tohoto připojení. Tak jako u jiných následujících služeb bude záležet především na schopnostech připojeného subjektu sám si vybudovat dané zařízení a pak jej nadále spravovat. V současné době je FW používán i jako součást zabezpečení v oblasti osobních počítačů (Personal Firewall).

Pro připojené organizace není lehké doporučit ten „nejlepší“ firewall. Každá organizace si sama musí rozhodnout, jaké vlastnosti, jaký výkon (zejména v propustnosti) po firewallu požaduje. Překlad adres a paketový filtr poskytují už i jednoduché firewally typu IPTABLES postavené na Linuxové platformě.

U centrálních firewallů snad více než u jiných služeb platí požadavek na vysokou dostupnost řešení, na možnost zvyšovat výkon v závislosti na zvyšujícím se provozu na síti ROWANet.

Na trhu je celá řada HW i SW řešení vyhovujících potřebám uživatelů ROWANetu, existuje i několik řešení splňující požadavky kladené na centrální firewally. Je ovšem otázkou, zda do silného centrálního firewallu investovat v první fázi projektu, kdy není jisté, zda připojované subjekty budou mít o takovou službu vůbec zájem a zda tedy vybudování silných centrálních firewallů nechat na komerčních subjektech připojených do ROWANetu. Odložení vybudování centrálních firewallů a jejich outsourcing doporučujeme.

5.2.2.2. Systémy detekce průniku

Systémy pro detekci průniku - Intrusion detection system (IDS) a Intrusion protection system (IPS) se v poslední době prosazují jako přirozený doplněk k firewallům při ochraně dat organizace. Prvky IDS umožňují odhalit útoky, které FW nezachytí. IDS jsou určeny především k pasivní ochraně, k logování a informacím o chování systému, IPS jsou navíc vybaveny moduly, které umožní konfigurovat automatickou reakci systému na detekovaný útok (například systém IPS může sám automaticky přestavit pravidla komunikace na firewallu, tak, aby dočasně přerušil probíhající útok).

Správně navržený systém slouží k ochraně nejdůležitějšího zdroje v systému jak před útoky zvenku i zevnitř. Obecně se prvky IDS systému dělí na dva typy: zařízení, které sleduje provoz na síti a zařízení, které sleduje aktivitu jednotlivého počítače. Kombinací síťových IDS a IDS pro servery dosáhneme vysokého stupně ochrany před neoprávněnými aktivitami. Porovnání Host a Network IDS uvádí následující tabulka.

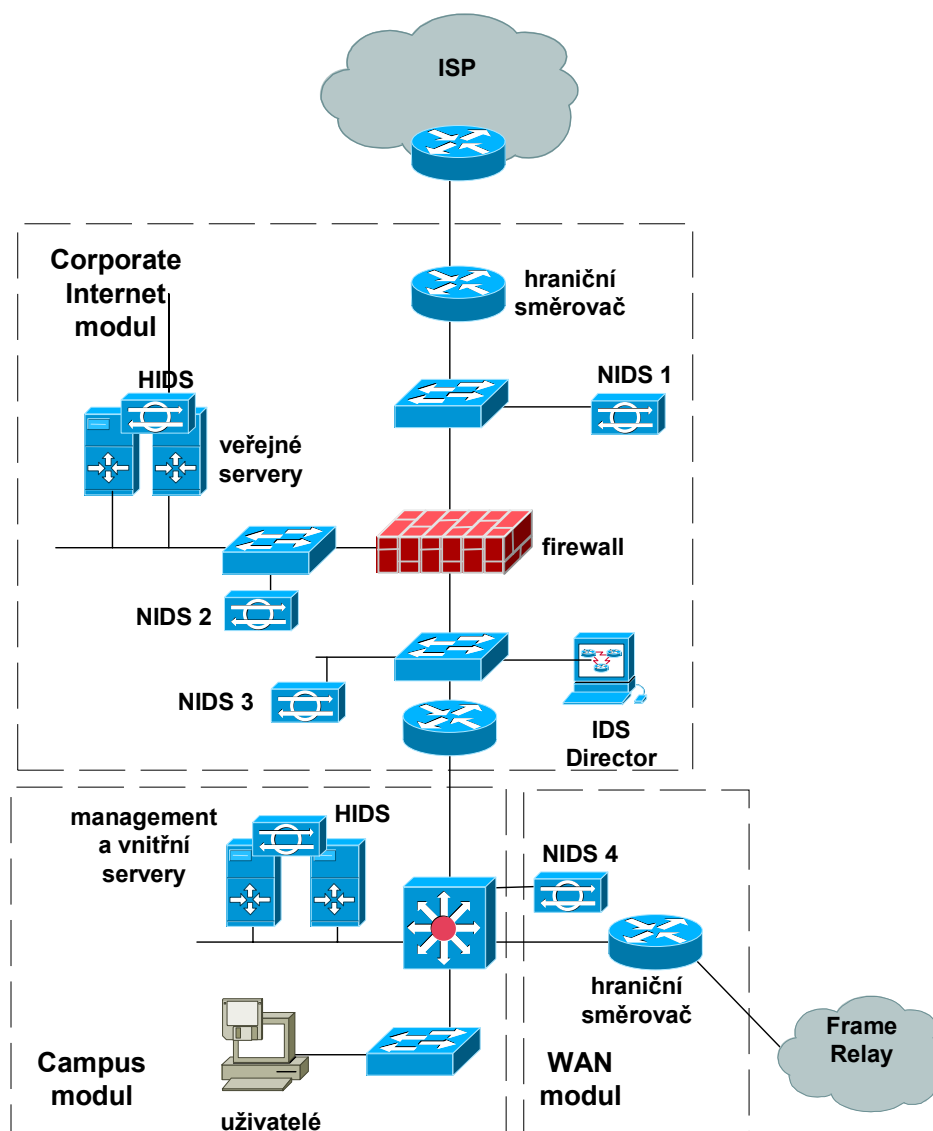
	Host-Based (HIDS)	Network-Based (NIDS)
+	Je schopen ověřit zda byl útok úspěšný či nikoliv. Funkčnost není ovlivněna propustností nebo použitím enkrypcce. Je schopen zabránit útoku.	Chrání všechny koncové stanice na monitorované síti. Neovlivňuje výkon koncových stanic/serverů. Je schopen detekovat DoS útoky.
-	Využívá zdroje serveru. Možnost použití závisí na OS. Rozšiřitelnost - vyžaduje instalaci jednoho agenta/serveru.	Náročnější implementace v prostředí přepínané LAN. Monitoring >1Gbps zatím problémem. Obecně neumí proaktivně zastavit útok.

Tabulka 5-1 Porovnání Host versus Network based IDS

IDS/IPS systémy využívají několik rozdílných přístupů k odhalování možných útoků. Základem bývá databáze signatur známých útoků. Databáze signatur je ve své podstatě hodně podobná databázi známých virů. Dalším možností je sledovat provoz, a vyhodnocovat komunikaci a protokoly, které nevyhovují normám RFC. Některé IDS systémy jsou schopny se vzdělávat, samy se učí charakteristiky „normálního“ provozu a upozorňují na odchylky od dříve naměřených hodnot.

Je více způsobů, jak konfigurovat automatickou reakci na detekovaný útok. Je důležité po instalaci vyladit systém tak, aby na straně jedné poskytoval maximální ochranu, ale na straně druhé, aby generoval co nejméně tzv. false-positive alarmů, tedy zpráv kdy systém IDS nesprávně detekuje normální provoz jako útok. Množství zpráv generovaných systémem nesmí přesáhnout únosnou mez, kterou administrátor systému je ještě schopen sledovat. Někteří odborníci automatickou odpověď na útok nedoporučují, protože tato vlastnost systému pak může být využita útočníkem k útokům typu DoS (Denial of Service).

Snad více než u jiných bezpečnostní prvků platí, že nestačí jednou nainstalovat, ale je potřeba průběžně sledovat provoz systému a vyhodnocovat hlášení generovaná systémem. Správná funkčnost IDS musí být podpořena pravidelným vyhodnocováním získaných informací a aktualizací systému. Jeden z možných způsobů nasazení IDS systému ilustruje následující obrázek.



Obrázek 5-2 Design sítě s ID systémy

5.2.2.3. Content filtering

Content filtering - filtrování adres URL, také známé jako filtrování obsahu, pomáhá minimalizovat nebezpečí, jemuž jsou sítě vystaveny ze strany www serverů nabízejících obsah, který může potenciálně způsobovat problémy.

Takové jsou například www servery se „závadným“ obsahem nabízející obsah infikovaný viry, nebo www servery obsahující návody na vytváření virů. Filtrovaní obsahu nejen posiluje bezpečnost sítě, ale pomáhá také zvyšovat produktivitu zaměstnanců připojené organizace, snižuje celkovou zátěž sítě.

Kontrolování obsahu funguje několika způsoby. Může být přímo omezen přístup na URL stránky uvedené na seznamu „zakázaných“ stránek. Některé systémy používají váhy, kdy vyhodnocují stránku z hlediska výskytu slov, umístění grafiky, odkazů na reklamní bannery atd.

Přístup k filtrování může být rozdílný – buď se přístup na stránky zakáže úplně, nebo je na některé povolen ve večerních hodinách, nebo se omezí rychlost přístupu na stránky. Přístup na stránky může být například povolen poté, co je uživatel dotázán, zda skutečně chce zobrazit „závadnou“ stránku s upozorněním, že jeho přístup bude zaznamenán systémem. Použití adresářových služeb pak umožňuje nastavit různá práva přístupu individuálně různým skupinám uživatelů.

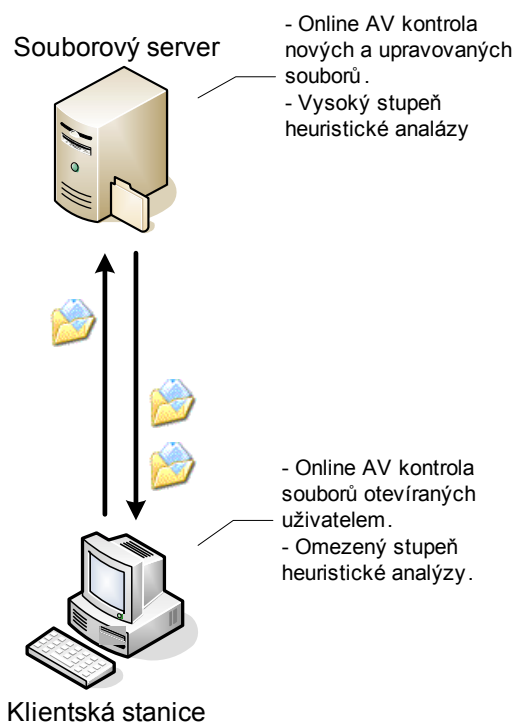
Dle našeho názoru je zavedení filtrování obsahu spíše „politický“ než technický problém, omezení přístupu je většinou uživatelů hodnoceno jako zásah do soukromí. Zavedení filtrování obsahu musí být podpořeno řídicími pracovníky, nejlépe pokud bude kontrola obsahu obsažena v bezpečnostní politice organizace.

Pokud bude v ROWANetu služba filtrování obsahu zavedena hned na začátku a jako podmínka využívání služeb připojení, bude akceptována. Později, po spuštění systému ROWANet, se bude jen obtížně hledat podpora pro její zavedení. Více než u jiných bezpečnostním prvků je zde nutno postupovat v souladu se zákony na ochranu osobních údajů.

5.2.2.4. Antivirová ochrana

Antivirová ochrana (AVO) je nejrozšířenější součástí bezpečnosti informačních systémů. V současné době je AVO implementovaná v nějaké podobě i na většině domácích počítačů.

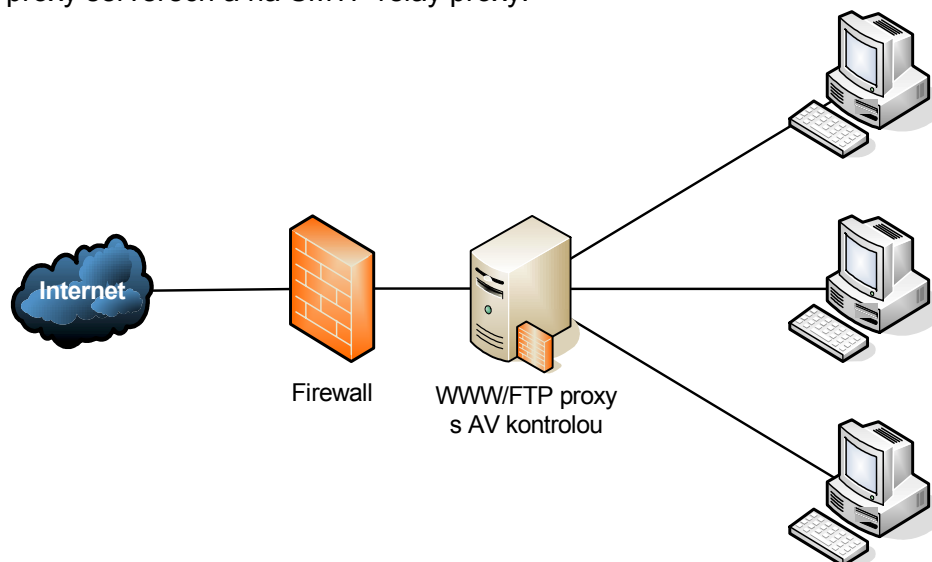
Vývoj v oblasti antivirové ochrany reaguje na nové trendy v šíření virových infekcích. Klasická ochrana proti virové infekci na úrovni souborového systému již nedostačuje, viru typu Slammer souborový systém ke svému šíření vůbec nepoužívají.



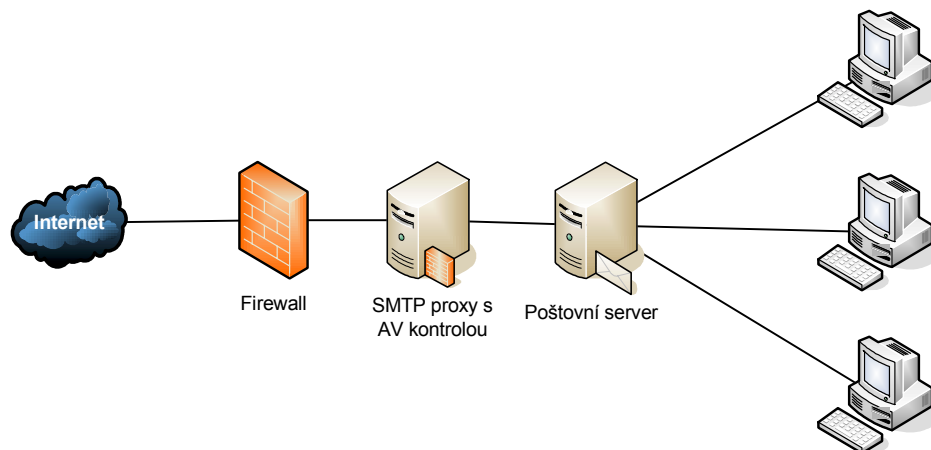
Obrázek 5-3 Příklad AVO souborového systému

K moderním trendům v AVO patří antivirová ochrana na vnějším perimetru organizace. Antivirovými produkty je kontrolována FTP, HTTP, SMTP komunikace ven a dovnitř organizace. AVO na koncových stanicích nestačí, správčové systémy většinou mají malou nebo žádnou kontrolu nastavení, nemají kontrolu nad aktualizacemi virových definic. Proto je nutno přidat AVO na centrálních serverech, kde nastavení je pevně v rukou správců sítě.

Následující dva obrázky ukazují příklady nasazení antivirové ochrany na www proxy serverech a na SMTP relay proxy.



Obrázek 5-4 Příklad AVO HTTP a FTP komunikace



Obrázek 5-5 Příklad AVO SMTP komunikace

5.2.2.5. Antispam

S nevyžádanou poštou se setkal již každý uživatel Internetu. Nevyžádaná pošta nejen že obtěžuje koncové uživatele, ale může způsobit i nepřiměřenou zátěž sítě. Navíc v současné době je e-mail nejoblíbenějším způsobem šíření virů.

Elektronická zpráva je spamem, **když** údaje o osobě příjemce a obsah zprávy jsou irelevantní, protože zpráva se dá rovnocenně podsunout mnoha dalším potenciálním příjemcům **a zároveň** příjemce neposkytnul ověřitelné, jednoznačné a vždy odvolatelné povolení k poslání zprávy **a zároveň** přenos a příjem zprávy se jeví příjemci jako poskytnutí neoprávněného prospěchu odesílateli.

Metody boje proti spamu jsou velmi různorodé a každý z nich přináší výhody i nevýhody. Vhodná kombinace těchto metod může snižovat množství nevýhod a zvyšovat účinnost antispamového řešení.

Filtrace podle adresy odesílatele

Nejjednodušší, ale také nejméně spolehlivou metodou je filtrování příchozí pošty podle adresy odesílatele. Výhodou je velmi snadná implementace do poštovního serveru i poštovního klienta. V dnešní době je ale tato metoda neúčinná. V současnosti spameři nejčastěji falšují adresu odesílatele a ve svých spamech uvádějí URL adresu, kde může „potenciální“ zákazník pokračovat.

Filtrování podle adresy SMTP serveru

Ještě před samotným zahájením přenosu pošty ze vzdáleného SMTP serveru si může přijímaná strana ověřit, zda odesílající server nepatří do skupiny serverů, které rozesílají (nebo jsou zneužity k rozesílání) spamy. Nejznámější dvě veřejné databáze jsou ORDB (Open Relay Databáze – www.ordb.org) a MAPS (Mail Abuse Prevention Systems – www.mail-abuse.org).

Databáze ORDB je poskytována zdarma a tato služba shromažďuje a posléze zveřejňuje seznam SMTP serverů, které nejsou chráněné proti rozesílání spamů. Databáze MAPS je komerční službou, která poskytuje několik seznamů, které může poštovní server využívat.

Výhodou těchto seznamů je snadná implementace do poštovního serveru. Další předností je ukončení případného přenosu spamu ještě před samotným odesláním, což šetří přenosové pásmo.

Nevýhodou těchto seznamů je malá flexibilita, kdy omylem vložený SMTP server je poměrně obtížné vymazat z těchto seznamů a po celou dobu může být pošta odesílaná z tohoto serveru blokována na straně příjemců.

Bayesiánský filtr

Bayesiánský filtr analyzuje obsah zprávy a klasifikuje ho mírou pravděpodobnosti, že daná zpráva je spam. Tuto činnost provádí na základě porovnání slov v obsahu zprávy s obsahem své databáze, kam zařazuje slova ze zpráv, které uživatel již dříve označil za spam nebo naopak za vyžádané zprávy. Z toho plyne, že filtr je třeba nejdříve „naučit“, tedy naplnit jeho databázi e-maily, o nichž sám uživatel rozhodne zda jsou či nejsou spamem.

Protože neexistuje jasná definice spamu a jednomu uživateli se stejná zpráva může jevit jako spam a druhému jako zajímavá obchodní nabídka, bayesiánský filtr je po instalaci buď prázdný nebo dodaný pouze se základními slovíčky (Viagra, sex, atd.) a poté jej musí administrátor doplnit.

Výhodou Bayesiánského filtru je vysoká míra identifikace spamu (pokud je naplněn „správnými“ slovíčky).

Nevýhodou je nutnost učení filtru po instalaci a poté průběžná aktualizace administrátorem poštovního serveru v čase tak, aby byl účinný proti novým stylům spammerů. Rovněž nevýhodou lze označit i nutnost příjmu spamů, aby mohly být následně vyhodnoceny. Nešetří tedy přenosové pásmo.

Filtrování podle statistiky vzdálených SMTP serverů

Doplňkovou metodou proti spamům je tvoření databáze se statistikou vzdálených SMTP serverů, které se snaží průběžně odesílat poštu pro lokální systém. Statistika může například shromažďovat údaje o počtu zpráv přijatých ze vzdáleného serveru za poslední hodinu, počet otevřených spojení v jednom okamžiku, počet neznámých adresátů v e-mailech, počet příjemců ve zprávě, atd.

Omezení pak mohou definovat maximální počet zpráv z jedné adresy za hodinu, maximální počet neznámých příjemců (ochrana proti útoku „directory harvest“), maximální počet příjemců v jednom e-mailu, atd. Pokud vzdálený server překročí dané limity (pokus o spamování), je na určitou dobu tento server odmítán lokálním poštovním serverem.

Jako naprosto antiproduktivní se ukazuje odpovídání na spam, případně kliknutí na odkaz „Odeberte mne ze seznamu adresátů“. Mnoho spamovacích robotů zkouší naslepo všechny možné kombinace názvů e-mailových schránek a takové kliknutí pak považují za potvrzení existence uživatele a zařazují jej do seznamu aktivních schránek. Takové kliknutí má tedy ve své podstatě za následek znásobení množství nevyžádané pošty.

V současné době antispamové produkty procházejí prudkým vývojem. Doporučujeme zatím vyčkat na nové verze programů i na úpravu legislativního rámce.

5.2.2.6. Autentizace a autorizace

Většinu bezpečnostních opatření lze implementovat mnohem efektivněji, pokud systémy vědí, „s kým mají tu čest“. Tedy kdo je ta osoba (nebo server) která k danému subsystému přistupuje (autentizace), jaká má tato konkrétní osoba práva k používání služeb subsystému (autorizace). Mnoho systémů vyžaduje i zpětný audit přístupů (accounting).

AAA systémy vyžadují, aby organizace měla přesně popsány pracovní postupy, vyžaduje popis funkcí a rolí. Nedostatečně jasně definované a nepopsané business procesy uvnitř organizace je častou překážkou úspěšné implementace AAA řešení.

Dobře navržené AAA systémy oddělují správu uživatelů od správy přístupových práv. Uživateli je po založení do systému přiřazena identita a této identitě několik rolí v závislosti na jeho pracovním zařazení. Práva přístupu jsou pak udělována rolím, ne jednotlivým uživatelům. Toto rozdělení umožňuje efektivní správu přístupových práv a zmenšuje prostor pro lidskou chybu. Nedílnou částí řešení musí být i způsob odstranění neaktivních uživatelů ze systému. Tzv. účty „mrtvých duší“ jsou jedním z častých způsobů útoků na organizaci.

Adresářové služby jsou řešením, který může být použit i pro vyřešení požadavků na AAA. Návrhu adresářových služeb je věnována samostatná kapitola.

5.2.2.7. PKI

Infrastruktura veřejných klíčů - Public Key Infrastructure (PKI). Termín PKI bývá používán ve dvou významech. První význam je používán při popisu metod, technologií a technik, které dohromady poskytují zabezpečenou PKI infrastrukturu. Druhý význam znamená použití páru klíčů (veřejného a privátního) pro autentizaci a pro šifrování obsahu zpráv.

PKI infrastruktura tedy

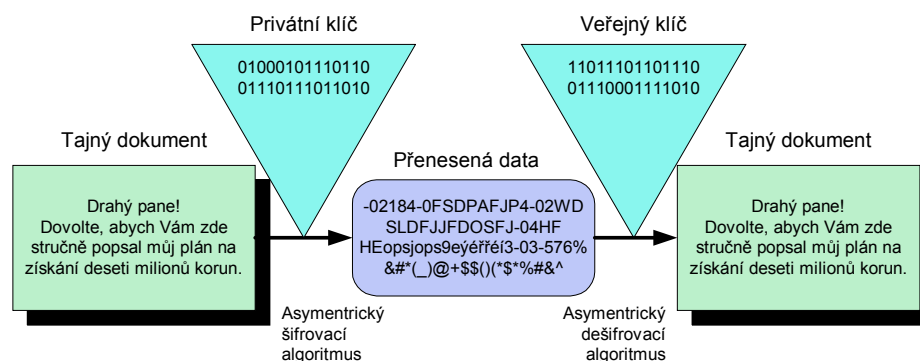
- Přijímá žádosti
- Vydává certifikáty
- Odvolává certifikáty
- Zpřístupňuje certifikáty (uživatelům/aplikacím) lokální CA

PKI infrastruktura nabízí uživatelům následující služby:

- Jistotu o kvalitě informace poslané a obdržené elektronickou cestou. Jinými slovy, že zpráva nebyla při své cestě k adresátovi nijak změněna.
- Jistotu o zdroji a cíli této informace, tedy že odesílatel je skutečně tím, za koho se vydává a že zprávu si přečte pouze adresát, kterému je zpráva určena.
- Nezpochybitelnost času, kdy daná zpráva vznikla, tedy funkce časových razítek.
- Jistotu o utajení informací obsažených ve zprávě.
- Možnost takto poslané informace použít při právních úkonech.

K tomu účelu PKI využívá matematickou techniku šifrování pomocí veřejného klíče. Při ní je použit pár vzájemně souvisejících šifrovacích klíčů pro ověření identity odesílatele (elektronický podpis) a/nebo k zajištění soukromí (šifrování). Veřejný klíč je publikován tak, aby byl přístupný všem, privátní klíč zůstává stále u jeho majitele, může být uložen například na čipové kartě uživatele.

Metodu šifrování ukazuje následující obrázek:



Obrázek 5-6 Příklad šifrované komunikace

Následující tabulka vysvětluje, kdy je použit privátní a kdy veřejný klíč při komunikaci dvou subjektů.

Funkce	Typ klíče	Čí klíč je použit
Zašifrování zprávy pro adresáta	Veřejný klíč	Adresáta
Podepsání zprávy	Privátní klíč	Odesílatele
Dešifrování obdržené zprávy	Privátní klíč	Adresáta
Ověření podpisu	Veřejný klíč	Odesílatele

Certifikáty vydané CA ROWANetu mohou sloužit například pro ověřování identity uživatelů přistupujících ke svým datům uložených na centrálních serverech, certifikáty mohou být použity pro komunikaci občanů s místními úřady.

Certifikační autorita může být postavena jak na komerčních produktech, tak i na Open Source řešení (OpenCA).

5.3. Popis základních infrastrukturních služeb IP sítě

V této kapitole se zaměříme především na návrh infrastrukturních služeb uvažované soustavy IP sítě.

Infrastrukturními službami IP sítě rozumíme několik dílčích distribuovaných aplikací, využívajících ke své činnosti protokol TCP/IP, které poskytují informace kritické pro funkci ostatních aplikací v prostředí sítě TCP/IP. Jsou to (v pořadí dle klesajícího významu) služby:

- DHCP – přidělování konfiguračních parametrů IP uzlům,
- DNS – adresářové služby pro prostředí TCP/IP,
- NTP – synchronizace systémového času,
- WINS – adresářové služby TCP/IP pro systémy MS Windows.

Tyto služby v dané rozsáhlé IP síti vždy tvoří jediný provázaný celek. V předkládaném návrhu je hlavní důraz kladen na efektivitu systému jejich poskytování, správy a využívání.

5.3.1. Návrh základní architektury služeb IP sítí

Uvažovaná komunikační infrastruktura KÚ Vysočina je z pohledu logické struktury (IP adresace, pravidla pro řízení komunikace apod.) tvořena propojenými vzájemně řízenými IP sítěmi participujících subjektů. Vzhledem ke skutečnosti, že v budoucnu není možno vyloučit vyčlenění jedné nebo více z těchto částí v podobě nezávislé IP sítě, je třeba tento princip respektovat i v návrhu systému poskytování infrastrukturních služeb. Zároveň je však nutno zohlednit (v obecné rovině protichůdný) požadavek na snížení ekonomické náročnosti řešení, zejména vytvořením předpokladů pro sdílení potřebných technických prostředků jednotlivými logickými složkami společné infrastruktury.

Přizpůsobení návrhu komunikační infrastruktury

Mimo základní požadavky na úroveň funkčnosti (dostupnost apod.) jednotlivých typů služeb stojí hlediska ekonomická. Zde jsou ve zjevném protikladu dvě možné koncepce:

- minimalizace nákladů na provoz komunikační infrastruktury,
- minimalizace nákladů na vybudování a správu soustavy služeb, resp. správu budované komunikační infrastruktury jako celku.

Pokud zvolíme jako primární hledisko úspory provozních nákladů komunikační infrastruktury, bude žádoucí provést investici do vybudování místních serverů soustavy služeb, popř. aplikačních serverů pro lokality disponující omezenou šířkou přenosového pásma.

Při opačném přístupu nelze vyloučit stav, kdy provozní náklady a zejména doba odezvy na některých užívaných přenosových trasách převyší ekonomickou výhodnost centralizace serverů soustavy služeb a aplikačních serverů.

5.3.2. Služba DNS

Obsahem této kapitoly je úvod do principu činnosti soustavy DNS, přehled z něj vyplývajících kritérií a zásad pro budování optimálně pracující soustavy. V další kapitole je potom obsažen výchozí návrh pro výstavbu soustavy DNS na komunikační infrastrukturou KÚ Vysočina.

Služba DNS je jednou z nejzákladnějších infrastrukturních aplikací nad rodinou protokolů TCP/IP. Je distribuovanou databází umožňující dynamické vyhledávání služebních informací potřebných pro správnou činnost dané sítě TCP/IP. Hlavními principy její výstavby jsou:

- využití síťových protokolů IP (UDP, TCP),
- architektura klient-server,
- distribuované uložení informací a delegace autority,
- mechanismy pro zabezpečení vysoké dostupnosti a výkonnosti služby.

Na informacích poskytovaných službou DNS jsou závislé prakticky všechny aplikace využívající pro svou činnost komunikační protokoly TCP/IP. Základními typy informací, které soustava dnes obsahuje, jsou:

- IP adresa uzlu daného jména ("přímé" vyhledávání),
- jméno uzlu příslušející dané IP adrese ("zpětné" vyhledávání),
- informace o serverech soustavy DNS,
- informace o serverech elektronické pošty.

Architektura DNS je však koncipována v širším rozsahu a umožňuje rovněž distribuci jiných typů údajů.

Soustava DNS povoluje, aby zobrazení přímého vyhledávání nebylo jednoznačné (jednomu jménu může náležet více než jedna IP adresa). Zobrazení zpětného vyhledávání je však vždy jednoznačné (zadané IP adrese je při zpětném vyhledávání přiřazeno vždy nejvýše jedno jméno).

Popsané principy činnosti systému DNS tvoří následující komplex souvislostí:

- zpětné vyhledávání by mělo správci sítě (uživatelé) poskytovat co nejužitečnější informaci o uzlu s danou IP adresou (např. vodítko pro jeho fyzickou lokalizaci při řešení chybových stavů),
- zpětné vyhledávání musí být jednoznačně konzistentní s primární strukturou přímého vyhledávání,
- struktura zpětného vyhledávání by měla co nejlépe vyhovovat způsobu rozdělení pravomocí pro přidělování IP adres tak, aby celková doba trvání řetězce úkonů: přidělení adresy -> registrace v přímé i zpětné struktuře DNS, byla co nejkratší.

Systém primární struktury přímého vyhledávání je proto třeba volit tak, aby co nejlépe vyhověl předchozím požadavkům.

Pomocné, sekundární struktury klíčů

Cílem zavádění sekundárních struktur pro přímé vyhledávání je vytvořit soustavy jmen s jiným řídicím pravidlem. Pro jejich existenci existují dva hlavní důvody:

- Specifický způsob využití komunikační technologie, který pro snadnou orientaci uživatelů vyžaduje, aby sekundární systém jmen vyjadřoval jinou informaci než tu, která určuje složení jmen v primární struktuře přímého vyhledávání (např. pro účely elektronické pošty uvnitř podniku vyhoví lépe soustava jmen podle jeho organizačního členění než podle topologie použité sítě).
- S cílem zjednodušit nároky na správu specializované aplikace může být výhodné zavést "plochý", striktně systematický "prostor" jmen pro podporu projekce do relativně náhodně obsazovaného prostoru IP adres. Projekce musí být založena na nějakém algoritmu, aby bylo možné ji provádět automatizovaně. Pro "lidského" uživatele by totiž používání takového plochého prostoru jmen bylo přinejmenším nepříjemné, ne-li zcela nezvládnutelné.

Autonomní nebo duální koncepce soustavy DNS

Soustavu DNS lze v prostředí privátní IP sítě budovat jako zcela autonomní, tj. nezávislou na veřejné soustavě DNS v celosvětové síti Internet. Privátní implementace soustavy DNS v tomto případě obsahuje úplné a aktuální informace o vnitřním prostředí TCP/IP. Je využívána všemi účastníky privátní sítě pro řízení vzájemné komunikace. Podmínkou správné činnosti autonomní soustavy je, aby obsahovala všechny nezbytné funkční prvky včetně tzv. "kořenových" serverů.

Je-li požadováno určité funkční propojení mezi privátní IP sítí a celosvětovou sítí Internet či dalšími privátními IP sítěmi (např. s využitím soustavy firewall), lze autonomní soustavu DNS rozšířit na soustavu duální. Toto rozšíření spočívá ve vybudování duplicitní soustavy DNS malého rozsahu v rámci veřejné soustavy v síti Internet či v rámci dalších privátních sítí. Duplicitní soustava obsahuje minimální množství informací nutných pro komunikaci mezi privátní sítí a Internetem či dalšími privátními sítěmi.

Autonomní resp. duální koncepce DNS dává na jedné straně možnost provozovat soustavu i bez existence přímého propojení s dalšími sítěmi, na druhé straně díky naprostému logickému oddělení obou částí přináší výhodu utajení informací o vnitřní struktuře privátní IP sítě. Tato skutečnost je významným přínosem z hlediska zabezpečení privátního prostředí proti neoprávněnému působení cizích subjektů.

Kořenové servery

Kořenové ("root") servery, jsou klíčovým prvkem každé autonomní soustavy DNS. Jedná se o autoritativní (primární a sekundární) servery DNS s autoritou pro tzv. kořenovou ("root") zónu s názvem ".". Kořenové servery mají ve srovnání s ostatními DNS servery v téže autonomní soustavě mírně modifikovanou funkčnost.

Hlavní úlohou kořenových serverů je poskytovat ostatním serverům pracujícím v téže autonomní soustavě kompletní informace o autoritativních serverech všech existujících domén první úrovně (domény "com.", "cz." atd.). Stojí tedy na vrcholu funkční hierarchie dané autonomní soustavy DNS.

Kořenové servery jsou počátečním bodem řešení každého dotazu vzneseného na danou soustavu DNS. Proto je seznam kořenových serverů pracujících v dané autonomní soustavě DNS důležitou (a současně jedinou apriorní) informací, kterou musí být vybaven každý další DNS server v téže soustavě.

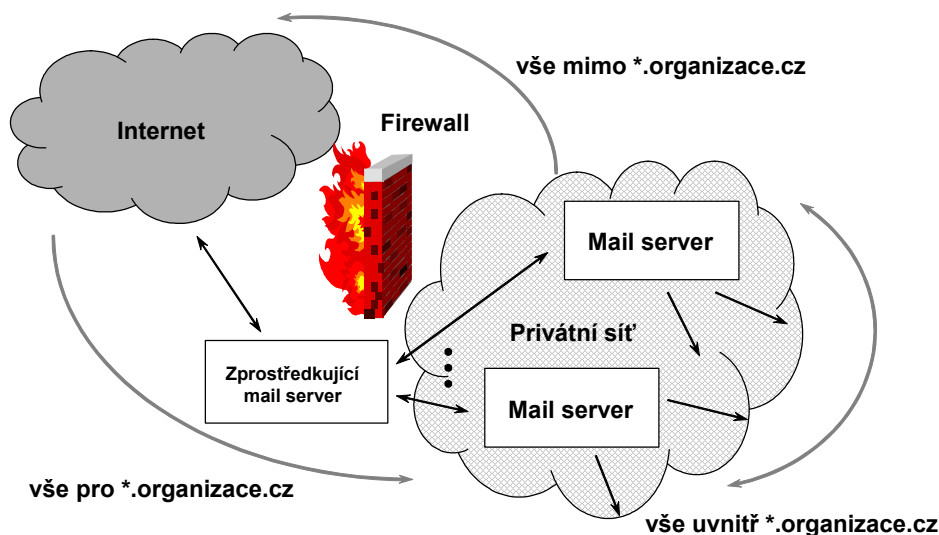
Souvislost DNS se systémem elektronické pošty

Systém elektronické pošty na bázi protokolu SMTP je těsně spjat s využíváním informací poskytovaných službou DNS.

Způsob směřování zpráv SMTP v prostředí izolované privátní IP sítě s duální soustavou DNS lze rozdělit do tří kategorií:

- přenos zprávy mezi libovolnými dvěma systémy náležejícími do privátní sítě (stejná doména organizace odesílatele i adresáta, např. "*.organizace.cz"),
- přenos zprávy ze systému ležícího vně privátní sítě na systém uvnitř privátní sítě,

- přenos zprávy ze systému ležícího uvnitř privátní sítě na systém mimo privátní síť.



Obrázek 5-7 Varianty směrování zpráv SMTP

V prvním případě jsou veškeré informace potřebné pro doručení zprávy SMTP dostupné oběma zúčastněným systémům ve vnitřní soustavě DNS privátní sítě. Činnost poštovní aplikace může být řízena soustavou DNS.

Ve druhém případě poskytuje systém DNS veřejné sítě vnější poštovní aplikaci pouze omezené množství informací. Vzhledem k oddělení obou sítí z důvodu zabezpečení je navíc vyloučena možnost přímého předání zprávy SMTP na cílový systém uvnitř privátní sítě.

Vnější systém DNS musí proto poskytovat takové informace, aby zpráva byla nejprve doručena na zprostředkující server elektronické pošty. Ten již bude oprávněn přistupovat k úplnému souboru informací vnitřního systému DNS, ale též navazovat přímou komunikaci se systémy uvnitř privátní sítě. Zmíněný zprostředkující server bývá typickou součástí soustavy "firewall".

Řešení třetí varianty přenosu zpráv SMTP je založeno na specifické konfiguraci vnitřních serverů elektronické pošty. Vnitřní servery nemají možnost doručit přímo zprávu určenou pro systém mimo privátní síť, neboť v prostředí izolované privátní sítě s duální strukturou DNS nemají přístup k informacím obsaženým ve veřejné soustavě DNS a z důvodu zabezpečení ani možnost navazovat přímou komunikaci se systémy vně privátní sítě. Poštovní aplikace na vnitřních systémech musí být proto konfigurovány takovým způsobem, aby zprávy s cílem určením mimo privátní síť (doména organizace adresáta různá než odesílatele, např. jiná než "*.organizace.cz") byly předávány vhodnému zprostředkujícímu serveru elektronické pošty. Tento server již musí být vybaven přístupem do veřejné soustavy DNS a možností navazovat přímou komunikaci se systémy vně privátní sítě. Obvykle se jedná o tentýž zprostředkující server jako ve druhé variantě.

Vhodnou konfigurací poštovní aplikace by vždy mělo být zajištěno, aby volba konkrétního poštovního serveru byla prováděna na základě informací poskytovaných soustavou DNS.

Zásady pro návrh a budování reálné soustavy DNS

Při návrhu implementace soustavy DNS je třeba brát v úvahu následující hlediska:

- srozumitelnost pravidel řídících princip členění jednotlivých soustav klíčů,
- organizační pružnost provádění změn v databázích,
- spolehlivost, dostupnost a výkonnost soustavy.

Výkonnost soustavy

Ke zvyšování výkonu soustavy DNS vede jak cesta omezování síťové komunikace, která je nezbytná pro nalezení odpovědi na dotaz vznesený DNS klientem, tak i cesta snižování výpočetní náročnosti, kterou pro autoritativní DNS server představuje vyhledání správné odpovědi v jím udržované databázi. Těchto druhů optimalizace je možno dosáhnout následujícími postupy:

- využíváním cache DNS serverů na lokálních sítích,
- umisťováním DNS serverů na systémy s velkou koncentrací síťových aplikací (servery elektronické pošty, servery WWW, servery jiných komunikačně orientovaných aplikací),
- realizací sekundárních autoritativních serverů v lokalitách "blízkých" klientům DNS, kteří intenzivně využívají právě informace ze zón na nich replikovaných,
- segmentací datového obsahu soustavy DNS na zóny malého rozsahu.

5.3.3. Systém DHCP

Služba DHCP je aplikací, jejímž cílem je vytvořit platformu pro plně automatickou konfiguraci základních komunikačních parametrů stanice a na ní provozovaných distribuovaných aplikací v síťovém prostředí TCP/IP. DHCP úzce navazuje na starší mechanismus BOOTP a zachovává s ním vysoký stupeň zpětné slučitelnosti.

Původním cílem definice mechanismu DHCP byla podpora v té době nového fenoménu v počítačových sítích TCP/IP – mobilních pracovních stanic. Dostatečně obecná architektura DHCP však přirozeně nalezla i další způsoby uplatnění a užívání tohoto prostředku se i díky masivnímu nárůstu počtu používaných mobilních stanic rychle rozšířilo.

Kompletní definice funkce systému DHCP je standardizována prostřednictvím RFC 2131 resp. RFC 2132. Vzhledem k relativně nedávnému vzniku uvedených standardů se však v praxi ještě často setkáváme s implementacemi, které splňují pouze starší definici mechanismu DHCP, RFC 1541.

Základními funkčními prvky systému služby DHCP jsou:

- DHCP server,
- DHCP klient,
- DHCP relay.

DHCP server

DHCP server je hlavním aktivním prvkem celého mechanismu. Slouží jako informační centrála pro distribuci zvolených konfiguračních údajů jednotlivým DHCP klientům. Tím se přirozeně stává i významnou součástí soustavy nástrojů pro správu počítačové sítě TCP/IP.

Z široké škály typů konfiguračních parametrů, které může server služby DHCP poskytnout klientské stanici, jsou nejdůležitější parametry pro primární aktivaci jejího TCP/IP stacku. Jedním z klíčových parametrů je tudíž i IP adresa pro klientskou stanici. Nalezení unikátní IP adresy a zabezpečení její rezervace pro danou stanici na dobu stanovenou správcem sítě, patří k základním a též nejčastěji využívaným schopnostem DHCP serveru. Mimo to může DHCP server plnit i celou řadu dalších doplňkových funkcí. Jejich soubor je závislý na konkrétním druhu implementace programového vybavení DHCP serveru.

DHCP klient

Klient služby DHCP je klíčovým subjektem mechanismu DHCP a též důvodem jeho vzniku. Jediným účelem nasazení služby DHCP je totiž poskytnout klientské stanici v komunikačním prostředí TCP/IP veškeré konfigurační údaje, které jsou zapotřebí pro její plnohodnotné začlenění do lokální počítačové sítě. Je zřejmé, že služba DHCP musí klientské stanici poskytnout minimálně nezbytné údaje potřebné k uvedení jejího TCP/IP stacku do normálního provozního stavu. Těmito údaji jsou:

- IP adresa,
- maska sítě,
- implicitní směrovač.

Tím však možnosti systému DHCP zdaleka nekončí. Klient DHCP může mimo údajů nezbytných pro zahájení komunikace na nejnižších úrovních TCP/IP obdržet též parametry pro konfiguraci vyšších transportních a aplikačních protokolů (distribuovaných aplikací), jako jsou DNS, LPD, NetBIOS a další.

Nejpodstatnějším aspektem na činnosti klienta služby DHCP je skutečnost, že k předání i užití všech poskytnutých konfiguračních parametrů dochází zcela automaticky, bez nutnosti jakýchkoli kvalifikovaných manuálních zásahů ze strany uživatele klientské stanice.

Podrobný výčet možností mechanismu DHCP je obsahem standardizačního dokumentu RFC 2131.

DHCP relay

Vzhledem ke způsobu primární komunikace mezi klientem služby DHCP a jejím serverem, je působnost serveru implicitně omezena na jedinou logickou podsít' TCP/IP. Aby v sítích TCP/IP s komplexnější topologií nevznikala nutnost zřizovat neúměrný počet samostatně pracujících DHCP serverů, byla do mechanismu DHCP zařazena též specifikace pro funkci "DHCP relay".

Účelem této pomocné služby je detekovat požadavky klientů DHCP, vznesené v těch částech topologie sítě TCP/IP, v nichž není přítomen žádný server DHCP. Relay musí dále požadavky transformovat do podoby, kterou je možno předávat v TCP/IP síti, a takto zpracované doručit tomu DHCP serveru, který je schopen poskytnout odpověď.

V praxi se s implementací funkce DHCP relay nejčastěji setkáváme u aktivních síťových prvků (směrovačů). Dostupné jsou však též implementace pro běžně používané univerzální operační systémy.

Zásady implementace služby DHCP

Vzhledem k poslání služby DHCP je zřejmé, že její dostupnost může zásadně ovlivnit provoz celé sítě TCP/IP. Dosažení vysoké provozní spolehlivosti systému DHCP, zejména prvků DHCP server a DHCP relay má proto pro trvalé udržení bezchybného provozu IP sítě kritický význam.

Jedním z nedostatků současné definice mechanismu DHCP, který je nutno v této souvislosti zmínit, je chybějící podpora pro zvyšování robustnosti implementace DHCP služby zřizováním redundantních (vzájemně se zálohujících) DHCP serverů. Překážkou tomuto postupu je neexistence mechanismu, který by serverům působícím v téže logické podsíti umožňoval sdílet informace o rezervovaných IP adresách. Tento zřejmý nedostatek je možné řešit dvěma způsoby. Obvykle je řešen implementací dvou DHCP serverů, jejichž konfigurace definuje shodný rozsah přidělovaných adres logické podsítě, avšak pravidlem „exclude“ vymezí rozsah adres, jež bude ignorovat. Tento rozsah je na primárním serveru definován tak, aby nekolidoval s rozsahem, jež ignoruje sekundární server a zároveň, aby rozsahy obou serverů tvořily celý rozsah adres logické podsítě.

Druhým způsobem je implementace clusterového řešení. V případě výpadku primárního DHCP serveru, převezme jeho službu záložní server disponující přesným obrazem konfigurace primárního serveru.

Oba způsoby je možné též kombinovat pro zvýšenou redundanci.

Vazba na službu DNS

Porovnáním základních funkcí služby DNS a služby DHCP snadno dospějeme k odhalení existujících souvislostí:

- konfigurační parametry klienta (resolveru) služby DNS mohou být distribuovány mechanismem DHCP,
- administrativní úkon přidělování IP adresy systémem DHCP by měl být neoddělitelně spjat s úkonem registrace stanice v systému DNS.

Je zřejmé, že ideálním stavem by byla automatická aktualizace informací v systému DNS na základě události představované uskutečněným dynamickým přidělením IP adresy systémem DHCP resp. vypršením doby platnosti dříve přidělených parametrů.

V praxi však zatím nacházíme jen velmi omezenou množinu implementací služeb DNS a DHCP, které by naznačeným způsobem komplexně pokrývaly celou oblast.

5.3.4. Základní principy časové synchronizace – NTP

Přesný čas

Standardní světovou časovou stupnicí užívanou pro měření času je Coordinated Universal Time (dále jen UTC). Časová stupnice UTC je odvozena z rotace Země kolem své osy. Je korigována vzhledem k času TAI (Internal Atomic Time) vkládáním přestupných vteřin v intervalu 18 měsíců. Stupnice UTC je však také nechtěně korigována například radiovými a satelitními navigačními systémy, modemy, či interními hodinami výpočetních zařízení.

Výpočetní zařízení, které pro korektní provoz vyžaduje přesný čas, jej může získat například pomocí Globálního polohovacího systému (GPS). Obvykle není možné vybavit každé zařízení vyžadující přesnou synchronizaci vůči UTC času přesným GPS přijímačem. Můžeme však vybavit jen jedno zařízení v roli časového serveru a synchronizovat jím zařízení spojená v síti. Zařízení musí podporovat některý ze síťových protokolů navržených pro distribuovanou synchronizaci časové informace, tedy protokol, který umí číst hodiny serveru, odesílat příslušné hodnoty klientům a korigovat jejich hodiny. Takovými protokoly jsou Network Time Protocol (NTP), Digital Time Synchronization Protocol (DTSS) a další.

NTP protokol

NTP - Network Time Protocol je protokol sloužící pro synchronizaci času klientského systému nebo serveru vůči jinému serveru, či referenčnímu zdroji přesného času, například radiovému a satelitnímu přijímači nebo modemu. Korekce času vůči UTC jsou při použití GPS satelitního přijímače v LAN prováděny typicky v rámci jedné milisekundy, v sítích WAN v řádu desítek milisekund. Zařízení podporující NTP protokol jsou obvykle hierarchicky organizována v NTP soustavách, na jejichž vrcholu poskytují přesnou časovou informaci dvě a více redundantně konfigurovaných NTP zařízení. Jedna úroveň se nazývá Stratum, Stratum-1 je nejvyšší úroveň.

GPS

GPS – Globální polohovací systém je systém pro určení přesné polohy a času a distribuci těchto údajů pomocí satelitů a rádiových vln. Systém je provozován Ministerstvem obrany USA. Poskytuje dvě úrovně přesnosti nazývané PPS – přesná polohovací služba a SPS – standardní polohovací služba. Zatímco služba PPS je kryptovaná a slouží pouze pro potřeby Ministerstva obrany USA a autorizovaných subjektů, služba SPS je veřejně dostupná.

Systém GPS je založen na přesném měření doby šíření signálů ze satelitů k přijímačům uživatelů. Signál šíří nominální konstelace jednadvaceti satelitů včetně tří záložních v šesti oběžných drahách 20000 kilometrů nad povrchem Země tak, aby v každém bodě na Zemi byl nepřetržitě dostupný signál minimálně ze čtyř satelitů. Pro korektní výpočet polohy přijímače a jeho časové odchylky od UTC musí přijímač získat signál ze čtyř satelitů zároveň. Všechny satelity jsou monitorovány kontrolními stanicemi, které určují přesné parametry oběžné dráhy a časovou odchylku atomových hodin satelitů. Tyto parametry jsou odesílány satelitům a jsou součástí navigačních údajů, které satelity přeposílají přijímačům uživatelů.

5.3.5. Adresářové služby

Adresářové služby jsou budovány na systému adresářových služeb standardů **LDAP** (Lightweight Directory Access Protocol).

„**Directory Services**“ je hierarchický informační prostor implementovaný na serverech jako centrální nebo distribuovaný systém, který je dostupný v celé síti. „Directory Services“ může implementovat například LDAP server. Ten ve své databázi obsahuje hierarchicky členěné „**entries**“ (položky), které obsahují „**attributes**“ (atributy). Atributy jsou určitým způsobem spárované hodnoty, které určují charakter „entries“.

Informace uložené v „directory“ mají charakter dat, které je třeba často hledat a méně často modifikovat. Databáze je proto navržena tak, aby právě vyhledání informace na základě atributů proběhlo v co nejkratším čase i při velkém objemu dat.

5.3.5.1. LDAP server

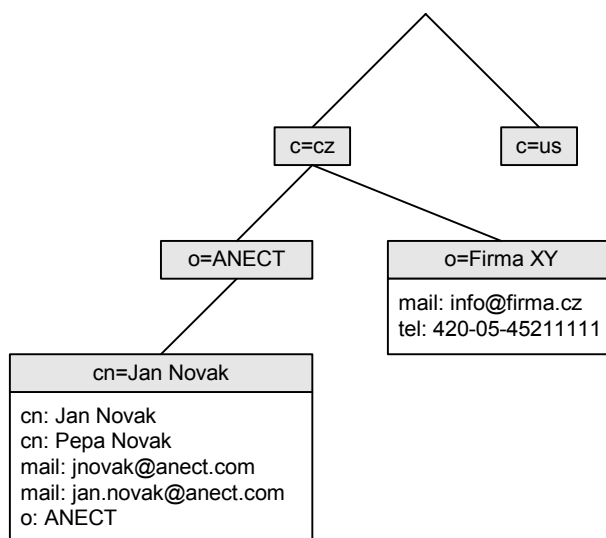
Jedním ze způsobů jak implementovat adresářové služby je LDAP server.

Atributy LDAP serveru obsahují informace o „entries“ – např. telefonní číslo, jméno, elektronickou adresu, a mohou být využívány aplikacemi (agent doručování zpráv MTA) i běžnými uživateli pro vyhledávání z klientského prostředí.

LDAP komunikace je navržena jako komunikace klient-server. Tj. na serveru je spuštěna služba, která obsluhuje LDAP databázi a reaguje definovaným způsobem na požadavky klientů. LDAP klient je dostupný uživateli a slouží jako uživatelské rozhraní proti LDAP databázi. Obdobným způsobem mohou LDAP server využívat aplikace. Jako příklad zde uveďme směrování zpráv mezi poštovními servery, nebo autentizace uživatelů.

5.3.5.2. Adresářový strom

Adresářový strom definuje hierarchii dat uloženou v LDAP databázi. Typický příklad hierarchie adresářového stromu popisuje následující obrázek.

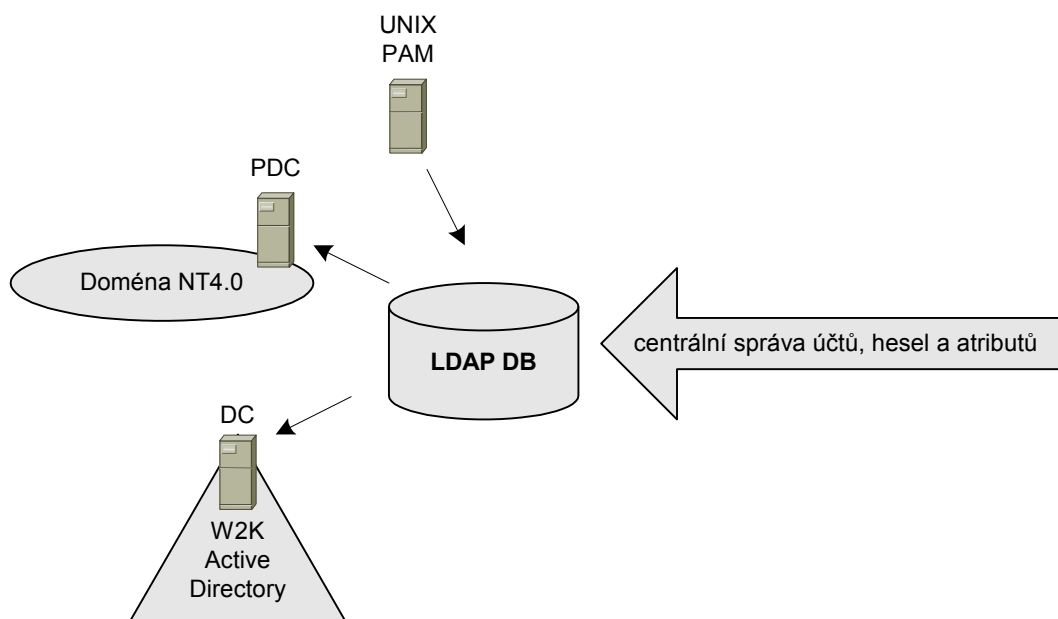


Obrázek 5-8 Příklad hierarchie adresářového stromu

LDAP umožňuje řídit používání atributů pro každé „entries“ pomocí tzv. „schématu“. Schéma se objektu přiřadí specifickým atributem - „objectclass“.

Je třeba upozornit na to, že uvedený příklad popisuje pouze jednu z mnoha možných variant hierarchického členění „entries“. Konkrétní strukturu je třeba navrhnout tak, aby:

- vyhovovala organizačním, geografickým (a jiným) potřebám organizace,
- byla kompatibilní s aplikacemi, které tuto strukturu využívají.



Obrázek 5-9 Synchronizace uživatelských účtů proti adresářové službě

5.3.5.3. Adresace položek

Každá položka je v databázi definována pomocí DN (Distinguished Name), které se skládá z RDN (Relative DN) a z cesty.

Pokud budeme uvažovat o názvech a struktuře položek z předchozího obrázku, bude mít „Jan Novak“ definovanou:

RDN: cn=Jan Novak a

DN: cn=Jan Novak, o=ANECT, c=cz.

5.3.5.4. LDAP databáze a ACL

LDAP prostředí definuje v hierarchickém stromě i aktualizaci položek a atributů.

Položky i atributy lze přidávat, mazat a modifikovat, a to v závislosti na definovaných právech k objektům. Nastavení práv se provádí pomocí ACL (Access Control List).

5.3.5.5. LDIF formát

LDIF (LDAP Data Interchange Format) je textový formát, který reprezentuje objekty v LDAP databázi.

Základní tvar formátu jedné položky v souboru LDIF je:

```
...
dn: <distinguished name>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
...
```

tedy například:

```
<LF>
dn: cn=Jan Novak, o=ANECT, c=cz
cn: Jan Novak
cn: Pepa Novak
mail: jnovak@anect.com
mail: Jan.Novak@anect.com
o: ANECT
<LF>
```

Následuje prázdný řádek a definice další položky LDAP databáze.

Více informací je v RFC 2252 a RFC 2256.

Pomocí nástrojů je možné provádět export/import data z LDAP databáze do LDIF formátu a naopak. Takto můžeme jednorázově naplnit LDAP databázi (například daty personálního oddělení), nebo naopak celou databázi odzálhovat do textového souboru.

5.3.5.6. LDAP schéma

LDAP schéma je definováno specifickým atributem „objectclass“. „Schema“ definuje seznam a typ atributů platných pro daný objekt.

Definice „schématu“ je součástí LDAP databáze a má následující tvar:

```
objectclass <jmeno_oc>
requires [seznam povinných atributů]
allows [seznam volitelných atributů]
```

Jako příklad zde uvádíme možné „schéma“ třídy objektů uživatel.

```
objectclass uzivatel
requires
    objectClass,
    ucet,
    heslo
allows
    telefon,
    kancelar
```

5.3.5.7. Bezpečná komunikace

Protokolem LDAP jsou veškerá data přenášena v tzv. "otevřené podobě".

Pro zajištění důvěrnosti přenášených dat se proto využívají technologie založené na zabezpečené komunikaci prostřednictvím certifikátů X.509. Jedná se o šifrování na úrovni TLS/SSL. Klient tak komunikuje s adresářovým serverem bezpečným protokolem LDAPS (což je analogie HTTPS).

5.3.5.8. Architektura adresářových služeb

Využití

Praktické použití adresářových služeb v síti KÚ lze shrnout v následujících bodech:

- Referenční databáze uživatelských účtů (a hesel) pracovníků KÚ - pro jednotnou autentizaci k "vnitřním" systémům a aplikacím.
- Databáze práv a rolí k "vnitřním" aplikacím - adresářové služby poskytnou informace pro autorizaci pracovníků KÚ k aplikacím provozovaných v ROWANetu.
- Distribuce (zveřejňování) certifikátů - prostřednictvím adresářové služby lze zveřejňovat certifikáty pracovníků KÚ tak, aby je mohli ostatní uživatelé použít například pro bezpečnou e-mail komunikaci nebo k autorizaci pracovníka pomocí jeho certifikátu.
- Adresářová kniha e-mailových adres - kontaktní báze pro e-mail komunikaci. Tato adresářová kniha může být využívána nejen uživateli poštovního systému, ale také samotnými MTA servery pro směrování zpráv.
- Údaje o uživateli všeobecného použití – telefonní číslo, číslo místnosti, budova, organizační útvar, funkce, atd.

Vnitřní a vnější adresářové služby

S ohledem na charakter informací, které bude adresářová služba obsahovat a s ohledem na jejich reálné využití a sdílení bude nezbytné uvažovat o dvou "nezávislých" adresářových službách s různým využitím a s různým datovým obsahem.

- Vnější adresářová služba pro spolupráci s externí subjekty.
- Vnitřní adresářová služba pro interní použití.

Na KÚ tedy vznikne vnitřní LDAP databáze, která bude obsahovat informace o pracovnících, kteří jsou přímo řízeni KÚ.

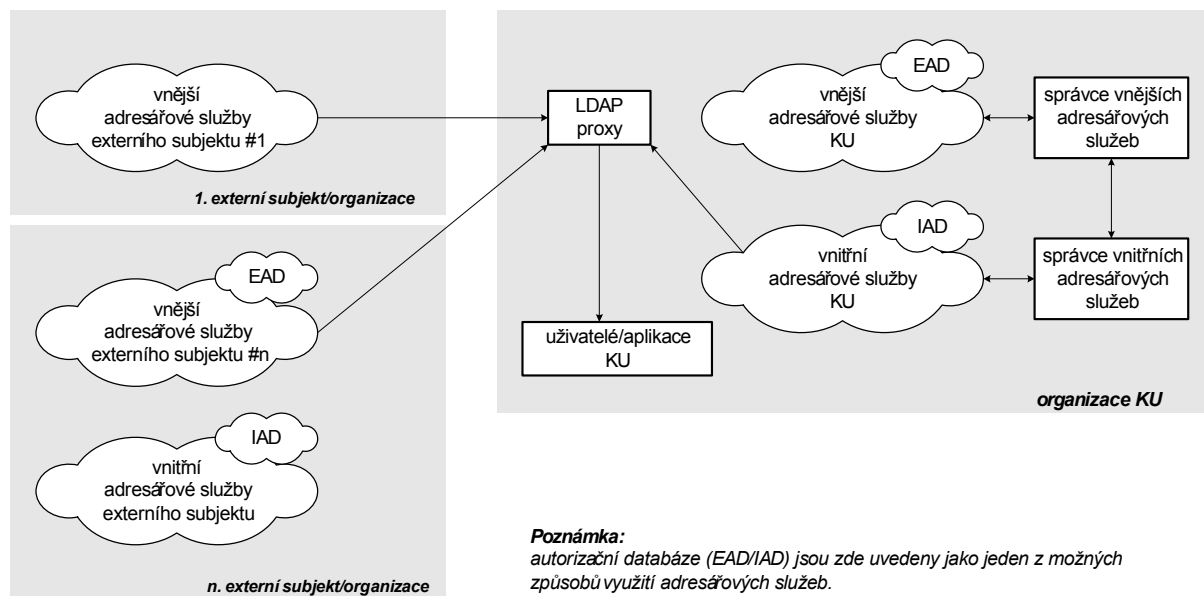
Dále bude provozována externí LDAP databáze, která bude sloužit pro autentizaci a autorizaci k externím aplikacím. V této adresářové službě jsou informace o pracovnících KÚ, které je třeba "zveřejnit" externím aplikacím, uživatelům, systémům.

Vazba mezi vnější a vnitřní adresářovou službou bude samozřejmě z pohledu správců obou databází umožněna např. automatickým importem / exportem dat (nebo filtrovanou replikací). Identita konkrétního pracovníka se tak může přes automatickou (nebo) potvrzovanou synchronizaci přenést z "vnitřního" do "vnějšího" adresáře.

Spolupráce adresářových služeb různých subjektů a organizací

Předpokládáme-li, že každý samostatný subjekt bude disponovat "vnitřní" i "vnější" adresářovou službou, bude jistě zajímavé vyřešit jejich vzájemnou spolupráci a vazby.

Principálně by spolupráce mohla fungovat dle následujícího logického modelu.



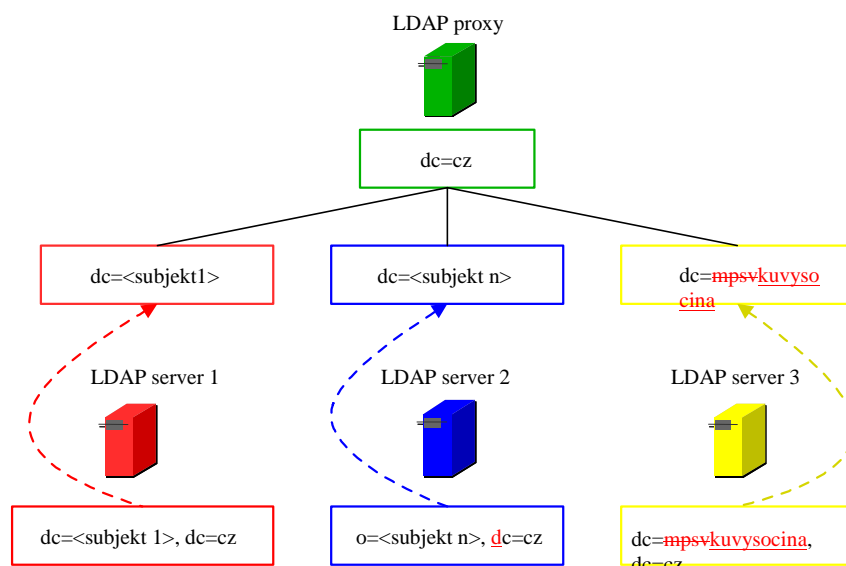
Obrázek 5-10 Logický model spolupráce adresářových služeb na KÚ

5.3.6. LDAP proxy jako integrační prvek adresářových služeb

V případě, že pro aplikace (nebo uživatele) KÚ potřebujeme získávat informace z více adresářových služeb (například z vnitřní AS KÚ a současně z externích AS jiných subjektů), lze vytvořit virtuální adresářovou službu.

Na obrázku je obecné schéma nasazení virtuálních adresářových služeb, která se chová jako LDAP proxy server. Ten v sobě shromažďuje data ze všech "podřízených" datových zdrojů.

LDAP proxy řeší časté problémy některých aplikací, které se neumí dotázat na více než jeden zdroj adresářových služeb.



Obrázek 5-11 Princip chování LDAP proxy

5.3.6.1. Hostování adresářových služeb

KÚ může externím subjektům nabídnout tzv. "hosting" adresářových služeb, tj. provozovat (zejména "vnější") adresářové služby externích subjektů včetně datového obsahu části LDAP stromu na zařízení(ch) na KÚ.

Důvodem k hostování může být například potřeba sdružit více serverů s "vnějšími" adresáři samostatných subjektů na jednom HW zařízení.

I v případě hostovaných adresářových služeb má ke správě dat přístup jejich "vlastník" - tj. správce z externího subjektu. Také způsob používání hostovaných adresářů externích subjektů zůstává stejný, jako v případě samostatných adresářových serverů, umístěných v lokalitách externích subjektů.

Za určitých podmínek lze uvažovat o hostování na stejném HW jako jsou externí adresářové služby KÚ.

5.3.6.2. Topologie adresářové služby

Zde uvedeme přehled nejčastěji používaných topologií adresářových služeb a doporučíme jednu z nich.

Centralizovaná adresářová služba s centrální správou

Pod pojmem centralizovaná adresářová služba budeme chápat následující topologický model služby:

- databáze je umístěna na jediném místě,
- služba je tedy dostupná pouze na jednom místě (prostřednictvím sítě je samozřejmě služba dostupná i z jiných lokalit),
- správa (aktualizace) databáze se provádí také na tomto jediném místě (prostřednictvím sítě je samozřejmě správa dostupná i z jiných lokalit).

Výhodou je snadná implementace, ale prakticky žádná odolnost proti výpadku služby. V případě, že data má využívat vzdálenější klient/aplikace, není zaručena dostupnost služby. Pro zvýšení dostupnosti centralizované služby je proto nutné použít techniku redundance nejen pro implementaci služby (např. clustery), ale i pro redundanci sítě (např. záložní linky).

Decentralizovaná adresářová služba s centrální správou

Tento model lze charakterizovat takto:

- Primární (master) databáze je umístěna na jednom místě, ze kterého se provádí správa dat.
- Další sekundární (slave) databáze jsou umístovány dle potřeby do různých částí sítě (lokalit) - služba je tedy plně dostupná z více míst.
- Data se jednosměrně synchronizují pomocí tzv. replik - z primární databáze do sekundárních.

Výhodou je snadná údržba konsistence dat a vysoká dostupnost služby prakticky v libovolné lokalitě. Data je však možné modifikovat pouze v primární databázi. Takové řešení snižuje nároky na redundanci infrastruktury.

Decentralizovaná adresářová služba s decentralizovanou správou

Tento model lze charakterizovat takto:

- Neexistuje primární/sekundární databáze - všechny databáze jsou s pohledu změn dat na stejné úrovni.
- Data se opět vzájemně synchronizují pomocí replik - tentokrát však je replikační algoritmus složitější, protože musí zohlednit situace, kdy byl objekt změněn na dvou místech současně.

Výhodou je vysoká dostupnost služby jak pro čtení tak, pro správu (modifikaci) dat. Tento model však předpokládá výskyt nekonzistentních situací, které je nutné následně řešit. Jako příklad zde uvedme situaci, kdy dva správci založí dva fyzicky různé uživatele se stejnou e-mail adresou. Přestože je v systému adresářových služeb požadována unikátnost atributu, obě databáze zjistí konflikt teprve po dokončení „synchronizace“.

S ohledem na předpokládané využití adresářových služeb doporučujeme, zejména z důvodů vysoké dostupnosti pro „čtení“ a zabránění vzniku konfliktů, použít v prostředí ROWANet „Decentralizovanou adresářovou službu s centrální správou“. Nezapomeňme však poznamenat, že i centrální správa umožní delegovat správu databáze (a jejich různých částí) na různé vzájemně nezávislé správce.

5.3.6.3. RFC

Pro lepší orientaci uvádíme přehled RFC, která definují použití LDAP prostředí v následující tabulce.

RFC #	Popis
RFC2307	An Approach for Using LDAP as a Network Information Service.
RFC2256	A Summary of the X.500(96) User Schema for use with LDAPv3.
RFC2255	The LDAP URL Format.
RFC2254	The String Representation of LDAP Search Filters.
RFC2247	Using Domains in LDAP/X.500 Distinguished Names.
RFC2164	Use of an X.500/LDAP directory to support MIXER address mapping.
RFC1960	A String Representation of LDAP Search Filters.
RFC1959	An LDAP URL Format.
RFC1823	The LDAP Application Program Interface.
RFC1558	A String Representation of LDAP Search Filters
RFC2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2.
RFC2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema.
RFC2596	Use of Language Codes in LDAP.
RFC2649	An LDAP Control and Schema for Holding Operation Signatures.
RFC2657	LDAPv2 Client vs.
RFC2696	LDAP Control Extension for Simple Paged Results Manipulation.
RFC2713	Schema for Representing Java(tm) Objects in an LDAP Directory.
RFC2714	Schema for Representing CORBA Object References in an LDAP Directory.
RFC2739	Calendar Attributes for vCard and LDAP.

Tabulka 5-2 Soupis RFC, která se vztahují k použití LDAP

5.4. Služby IP sítě nezbytné pro počáteční provoz infrastruktur

5.4.1. DNS

DNS je v podstatě jedinou službou, kterou je potřeba vybudovat v síti ROWANET hned od počátku. Pro provoz uvažovaných infrastruktur je od počátku nezbytné vybudování soustav služby DNS, tedy služby překládající v TCP/IP síťovém prostředí názvy infrastrukturních uzlů a služeb na IP adresy a naopak. Služba bude v rozsáhlých sítích nezbytná pro propagaci jmenného prostoru dané sítě do sítí dalších. Na tuto propagaci spoléhají další navázané infrastrukturní služby, zejména elektronická pošta a protokol SMTP zajišťující přenos zpráv elektronické pošty. Poštovní zprávy jsou uzly komunikujícími protokolem SMTP směrovány dle příslušných DNS záznamů až k cílovému příjemci poštovní zprávy.

Dalšími službami, jejichž funkčnost je zásadním způsobem závislá na propagaci jmenného prostoru (zejména mezi veřejnou celosvětovou sítí Internet a neveřejnými sítěmi) jsou služby WWW, poskytované především protokolem HTTP. Praktická dostupnost WWW služeb je při jejich množství v rozsáhlých sítích (jakou je například i veřejná celosvětová síť Internet) determinována organizací jmenného prostoru DNS službami.

5.4.2. NTP

Služba NTP je službou, kterou lze vybudovat bez dalších mimořádných nákladů. Ač ji nelze považovat za nezbytnou, její dostupnost v síti značně ulehčí synchronizaci času, jež je důležitá například pro správu a dohled sítí i pro další vyšší služby.

5.4.3. Firewall

Pro první fázi postačí pro poskytovatele libovolný firewall s překladem adres a paketovým filtrem. Tento firewall bude mít za úkol chránit před vnějším nebezpečím DNS a NTP servery, není tedy od něj potřeba vyžadovat žádný extrémní výkon.

Požadavky na takovýto firewall splní libovolný linuxový stroj nebo lze uvažovat i o SOHO (Small Office/ HOMe) zařízeních.

Pro zvýšení bezpečnosti by bylo vhodné doplnit tento firewall antivirovou kontrolou a prvky IDS.

Firewally připojených subjektů mohou být libovolného typu, od malých SOHO zařízení přes Open source až po komerční firewally typu CheckPoint, Netscreen nebo Pix.

5.5. Budování dalších služeb IP sítí

Aktivitu v dalších službách navrhujeme přenechat komerčním i nekomerčním subjektům připojeným do ROWANetu. Jednak se tím sníží zátěž na poskytovatele, jak finanční tak personální, a jednak bude vznikat pouze to, co uživatelé sítě ROWANet skutečně využijí. U většiny výše popsaných služeb lze mít vedle sebe více nezávislých poskytovatelů stejné služby.

Služby, o které zřejmě bude zájem:

- PKI
- Webhosting, serverhosting
- Zdroje definic AVO programů
- Poskytování prostoru pro e-mailové schránky
- Adresářové služby

Pro bezpečnost ROWANETu bude vhodné síť a důležité servery vybavit prvky IDS.

Centrální content filtering, centrální AVO ani centrální firewally v první fázi navrhujeme nebudovat.

6. Aplikační vrstva

6.1. Informace

Poskytování a sdílení informací – poskytování obsahu je jedním ze základních hybatelů společnosti jak na úrovni společenské tak i na úrovni ekonomické (obchodně - podnikatelské). Řada práv a povinností souvisejících s právem na informace je legislativně ohraničena jak zákony ČR a EU, tak i různorodými pravidly chování organizací, podniků, norem, programů, aktivit, sdružení atd. Proto budou stimulační a usnadnění realizace procesů i poskytnutí kvalitních nástrojů souvisejících se zpřístupňováním obsahu technickými prostředky ICT patřit k podpurným nástrojům rozvoje kraje Vysočina přesně v rámci teze „kraj, kde se dobře žije a podniká“.

Pro stimulaci vzniku a zpřístupnění obsahu je třeba řešit následujících oblastí:

Funkční požadavky:

- řízení publikování,
- vazba a klasifikace dat – sémantika informací,
- oborové, fulltextové, asistované vyhledání,
- grafická on-line, off-line prezentace obsahu.

Realizační požadavky:

- snadno, rychle – stimulovat kreativitu co nejširšího spektra subjektů,
- levně, opakovatelně – stimulovat kvantitu a pestrost,
- koncepčně – udržet technologický krok a integritu prostředí.

Prostředky:

- komunikační infrastruktura a její služby,
- sdružená komunikace – hlas, data, video,
- weby, redakční systémy, portály, databáze,
- podpora vzdělávání a užití prostředků a služeb ICT.

6.2. Zábava

Volný čas a jeho aktivní využití je životním trendem moderní společnosti. Možnosti a kvalita nabízených informací a služeb v této oblasti ovlivňuje např. volbu místa trávení dovolené nebo rozhodování o místě trvalého bydlení. Využití potenciálu nabídky těchto služeb na úrovni kraje i dílčích subjektů (organizací, podnikatelů, obyvatel) pro propagaci a rozvoj kraje Vysočina lze rozdělit do oblastí:

- informovanost o akcích, událostech a programech pro občany kraje (kultura, sport, zájmy, kroužky, ...),
- informováním o možnostech turistiky a rekreace v kraji (cykloturistika, agroturistika, chaty, chalupy, tábory, sportoviště, ...), včetně aktivního přístupu (ceníky, rezervace).

A to jak z pohledu:

- „chci svůj čas někde trávit – bavit se“,
- „chci akce pořádat – bavit ostatní“.

6.3. Vzdělávání

Úroveň vzdělání determinuje úroveň společnosti – regionu, určuje možnosti a pravděpodobnost úspěchu ve společensko-ekonomickém prostoru. Vzdělání však nelze zabezpečit prostým zpřístupněním a využíváním prostředků ICT. Vzdělání je postupný proces vedoucí ke znalosti jak uplatnit dostupné informace (lépe zpřístupněné pomocí ICT) v běžném podnikatelském či osobním životě ku prospěchu jedince, organizace či společnosti. Proto lze intenzivnější využívání ICT chápat jako jeden z možných podpůrných nástrojů, nikoliv jako nutnou či postačující podmínku. Role ICT v této oblasti má především význam v kvalitativně lepším přístupu k informacím ve smyslu – snadněji, rychleji, širšímu spektru posluchačů, z více oborů a s širším obsahem.

Také nově projednávaná legislativní norma - školský zákon - klade velký důraz na angažovanost konečných subjektů – škol a učitelů, proto rozvoj regionálních vzdělávacích center které:

- nabídnou lepší informovanost veřejnosti o kvalitě a rozsahu nabízených služeb (ve srovnání s ostatními kraji ČR a regiony EU),
- zabezpečí komunikaci a sdílení znalostí v rámci odborné veřejnosti (ředitelů, učitelů, žáků, rodičů),

bude hrát významnou roli. Jedním z technických způsobů jak tyto centra realizovat je využití prostředků ICT vzhledem k jejich pružnosti, rychlosti, dostupnosti, pestrosti (text, obraz, video, hlas) a relativně snadné dostupnosti (PC, připojení k internetu atd.). Dalším - lidským faktorem hovořícím pro intenzivnější využití prostředků ICT je jejich široká akceptace a přitažlivost pro mladou generaci. Nicméně vzdělání není vyhrazeno pouze pro tuto skupinu, obecně hovoříme o celoživotním vzdělávání a podpoře schopnosti společnosti absorbovat regionální i globální směry vývoje či výkyvy trhu – poptávky pracovní síly.

Naznačení možných technických způsobů realizace – nástrojů, norem a metodik je nastíněno v následujících sekcích této kapitoly.

6.4. Způsob realizace

6.4.1. Weby a portály

Jsou základním nástrojem pro řízenou distribuci informací centralizovanými prostředky – servery směrem k standardizovaným klientům – web prohlížečům poskytovaným nad protokolem HTTP(S).

Přímo v rámci kraje je provozována celá řada webů a portálů (občanů, obcí, organizací, státní veřejné správy, podniků atd.) a vzhledem k faktu, že internet není geograficky omezen, jsou běžně dostupné i další zdroje. Téměř ve všech případech se však jedná o izolované informatické zdroje bez vzájemné datové a logické návaznosti (kromě „linků“) zprostředkující informace především mimoregionálního charakteru.

Proto, vzhledem k faktu, že:

- internetové stránky s lokálním zaměřením mohou uživatelům nabídnout atraktivnější údaje,
- obsahem projektu je návrh komunikačního prostředí v jehož rámci budou v regionu kraje Vysočina distribuovány informace a poskytovány služby ICT,

je vhodné v rámci systémového projektu naznačit cestu jak budovat, umístit a provozovat regionální servery, kdy cílem takto budovaných regionálních serverů bude především nabídnout (v souladu s programem e-Europe):

- moderní on-line veřejné služby,
- dynamické prostředí pro e-business.

Hlavní problémy, jenž určují životaschopnost takového záměru, jsou:

- kvalitní obsah,
- finance na start a provoz projektu,
- technická realizace – HW, SW, KI, regionální generické a bezpečnostní služby.

Obsah

Internet, portály a weby nabízejí relativně bezproblémovou dostupnost nejrozličnějších druhů dat a služeb z kteréhokoli konce světa, v jakémkoli jazyce. Pro rozvoj kraje Vysočina je však hlavním obsahovým přínosem možnost vytvořit prostředí pro předávání informací a zpřístupnění služeb zcela opačného charakteru - v rodném jazyce, lehce dostupný obyvatelům kterékoliv obce běžně i jinou formou než elektronickou. Možnost využít služeb a seznámit se s:

- rozhodnutími lokálního zastupitelstva,
- vyřídit základní agendu (místní poplatky, osobní doklady, motorová vozidla, daně, atd.),
- informacemi v oblasti zdravotní péče (lékárny, pohotovostní lékárny, všeobecní a odborní lékaři, adresy, dopravní spojení, ordinační hodiny, objednávky atd.),
- informacemi v oblasti vzdělávání (jesle, mateřské školy, základní školy, střední školy, odborné školy, církevní, podnikatelské školy atd., adresy, dopravní spojení, možnosti ubytování, náplň výuky, dny otevřených dveří, třídní schůzky, omluvenky atd.),
- nabídkou pracovních příležitostí,
- nabídkou veřejné knihovny včetně rezervace,
- programem koncertů, divadel, kin, zábav včetně rezervace,
- atd.

Umožnit přístup z domova, z práce, spolu s vysokou mírou znalosti prostředí a vztahů, o nichž se v takových zprávách referuje nebo které služby nabízejí, jsou hlavní přínosy těchto serverů s regionální tematikou. Je logické, že pro uživatele jsou atraktivnější a bližší zprávy i služby týkající se okolí, v němž žije a pracuje, než nabídka "celostátně" či „celosvětově“ zaměřených zpravodajských, informačních a dalších serverů.

Vzhledem k šíři a pestrosti redakce daných internetových projektů nezajišťují obsah výhradně svými silami. Naopak kooperují navzájem, sdílejí informace a propojují služby. V praxi se u všech kromě původních - vlastních zpráv, služeb setkáme:

- s informacemi zpravodajských servisů agentur či jiných médií obecnějšího či širšího zaměření (např. iDnes, ČTK, státní, krajské, obecní zastupitelstvo, spolupráce s regionálními „klasickými“ deníky atd.),
- spoluprací externích subjektů vytvářejících virtuální redakční tým (zástupci nemocnic, škol, neziskových organizací, podnikatelů, reklamních agentur, pracovních agentur atd.) komunikujících v rámci integrovaného redakčního systému, který zabezpečuje řízený proces publikace,
- propojováním dílčích systémů např. pomocí webových služeb.

Finance

Oblast financování je velmi problematická a lze ji rozdělit do dvou základních oblastí:

- Kapitál na start projektu – zahrnující investice na HW a SW vybavení, zabezpečení konektivity do internetu, realizační programové a redakční práce. Danou problematiku lze řešit dvěma možnými přístupy:
 - Pokrýt vstupní náklady vlastními silami u subjektů s jinou – hlavní podnikatelskou činností. V tomto případě je skupina možných zřizovatelů značně omezena, může být omezen rozsah i kvalita celého projektu (řada služeb může mít tendenci –komerční charakter).
 - Připravit na úrovni kraje (vlastními prostředky či prostředky získanými z grantů a projektů EU) takové prostředí – technologicky a metodicky jenž umožní rychlý start projektu tj. zabezpečit generickou konektivitu, provozní prostředí (např. nástroji OpenSource či poskytnutím zdrojů centrálních – server a webhosting) a umožní se novému provozovateli zaměřit úsilí primárně na obsah a poskytované služby.

Nejvhodnějším způsobem se logicky jeví vyvážená kombinace obou výše zmíněných přístupů.

- Kapitál na provoz projektu – za základní možné zdroje pro dlouhodobé financování provozu lze identifikovat:
 - spolupráci s krajem, radnicí,
 - sponzorské aktivity,
 - zpoplatňování publikovaného obsahu,
 - reklamní aktivity,
 - off-line služby na principu provizí – rezervace ubytování, kulturních nebo sportovních aktivit, realizace marketingových průzkumů, zpoplatnění behaviorálních dat (hledaná hesla, nejčtenější příspěvky, nejvyužívanější služby, rozbor publika atd.).

Pro úspěšný start a následný rozvoj (vzhledem k současným technicko ekonomickým podmínkám v regionu) se jako nezbytně nutná jeví přímá, aktivní, technická i finanční účast regionu – zastupitelstva kraje a obcí. Důraz v první fázi musí být kladen na pestrost – přitažlivost služeb pro co nejširší spektrum uživatelů – občanů. Rozvinutí a akceptace tohoto způsobu nabídky a konzumace služeb zabezpečí i jejich přitažlivost pro organizace a podniky které se stanou v druhé etapě primárním zdrojem finančních prostředků.

Technická realizace

Podaří-li se vydefinovat obsah – co má být na portálech a webech, podaří-li se zabezpečit finanční prostředky na start a provoz je v neposlední řadě nutné znát cestu technické realizace daných projektů.

Technicky řešené oblasti lze rozdělit na:

- informační servis – on-line prezentace informací o službách, událostech, aktivitách atd.,
- off-line interakce – zpřístupnění elektronických formulářů,
- on-line interakce – obousměrná aktivní interakce založená na autentizaci uživatele a jeho autorizaci k provádění aktivit a úkonů (např. rezervace, podatelna),
- transakce – provázání systémů, logická návaznost a konzistence (např. vyřízení případu, rozhodnutí a doručení (platba).

Informační servis:

- řízená publikace, změna a stažení příspěvku v rámci redakčního systému,
- ukládání příspěvků na úložiště – databáze, souborový systém,
- oddělení obsahu a formátu,
- sdílení obsahu – syndikace,
- klasifikace informací – příspěvků dle daných pravidel, skupinou parametrů (např. dle DCMI).

Off-line interakce:

- transformace strukturovaných informací (html, db dat atd.) do přenositelného, obecně používaného formátu – pdf,
- jednoduchý a ekonomický tisk („print friendly version“) strukturovaných informací (html, db dat atd.).

On-line interakce:

- registrace uživatele,
- autentizace uživatele (jméno/heslo, El.podpis, certifikáty),
- autorizace uživatele,
- zpětné ověření a monitoring aktivity,
- integrace e-mail služeb,
- zabezpečený přenos (https).

Transakce:

- definovat transportní datové rozhraní – formát, sémantiku, zabezpečení a transportní protokol,
- definovat rozhraní volání služeb formát, sémantiku, zabezpečení a transportní protokol,
- zabezpečit technicky proces přenosu přímo nad protokoly a službami sítě („point to point“) nebo transportními („messaging“, „web service“) systémy (kontrolovaně, „one to many“, „many to one“).

Z výše uvedeného výčtu vyplývá, že technická část je rozdělena do dvou hlavních oblastí:

- definice pravidel a rozhraní (včetně návodů a příkladů) – systémová úroveň,
- realizace a provoz systémů – centralizovaných služeb např. podatelna, registry služeb, autentizační služby atd. – technická úroveň.

Tato oblast je pro další rozvoj služeb nad KI naprosto klíčová. Lze doporučit její detailní zpracování v rámci separátního systémového projektu.

6.4.2. Vyhledávací služby

Nejen tvorba a prezentace informací je důležitá, důležitým aspektem je i dohledatelnost – rychlost a přesnost získání požadovaných informací. Pro odborný odhad potřeb a priorit nám může posloužit např. průzkum realizovaný Centrem pro elektronický obchod společně s výzkumnou agenturou TNS Factum, který se zabýval využitím nástrojů e-Governmentu mezi podnikateli. Výsledky v oblasti vyhledávání informací lze stručně shrnout takto:

Většina dotázaných, kteří se průzkumu zúčastnili (cca 80 %), představuje „poučenou podnikatelskou obec“, která ví, na jaké stránky konkrétně jít a/nebo které z vyhledávačů či katalogů pro hledání informace použít. Konkrétně podnikatelé vyhledávají těmito kanály:

1. na internetu, hledáním na internetu, stylem „pokus/omyl“ – 23 %
2. na internetových stránkách příslušné instituce - 20 %
3. www.seznam.cz, na seznamu, seznam - 16 %
4. www.portal.gov.cz, portál veřejné správy – 15 %
5. www.businessinfo.cz, BusinessInfo- 6 %

Pro účely tohoto systémového projektu – potřeby kraje Vysočina lze vyvodit tyto důsledky:

- Je nezbytně důležitá klasifikace všech informací a správná sémantika webu.
- Registrace a indexace obsahu pomocí veřejných a známých vyhledávačů (Google, Alltheweb, Altavista, Seznam, Centrum, Atlas, Jyxo, Morfeo atd.).
- Registrace subjektů v katalogích portálů (především českého internetu -Seznam, Centrum, Atlas atd.).
- Správné strukturování informací (řazení do sekcí, témat atd.) na samotných webových stránkách projektu (ergonomie webu).

- Zabezpečení fulltextového prohledávání v rámci webových stránek těchto projektů.
- Provázání on-line informačních částí dílčích regionálních, republikových a evropských projektů formou syndikace obsahu. Poskytnutí krátkých zpráv oborovým webům a portálům – např. oblast školství (www.ceskaskola.cz atd.). Poskytnutí krátkých zpráv specializovaným webům a portálům zaměřeným např. na agregaci zpráv (www.pravednes.cz atd.).
- Zabezpečení přístupu k informacím – krátkým zprávám off-line pomocí klientských aplikací – RSS čtečky atd.

Všechny výše zmíněné kroky by ve svém důsledku měly zvýšit návštěvnost, oblíbenost, snadnost používání a tím pádem zabezpečit:

- reálnou využitelnost publikovaných informací a služeb v praxi – smysluplnost aktivit,
- atraktivnost těchto projektů pro komerční subjekty tj. zabezpečit dostatek finančních prostředků pro provoz a další rozvoj (formou sponzoringu, reklam, off-line aktivit atd.).

7. Správa systému, řízení a poskytování zdrojů

Vzhledem k finanční, technické a odborné náročnosti, která souvisí s vybudováním provozní infrastruktury a zabezpečením jejího chodu, je vhodné nabídnout možnost sdílet technické prostředky – zabezpečit a provozovat je centrálně, nabídnout či pronajmout je konečným subjektům, které se zaměří na tvorbu a nabídku obsahu – informací a služeb.

Základní způsoby spolupráce (podpory) lze rozdělit na:

- webhosting,
- serverhosting,
- outsourcing.

Všechny zde zmíněné způsoby poskytování prostředků a služeb (za poplatek i bezplatně - s určitým omezením či limitovanou formou) již ve světě internetu a v ČR existují. Mezi základní výhody a důvody proč je realizovat na úrovni kraje patří zejména následující skutečnosti:

- Takto provozované centrální služby lze s výhodou „předkonfigurovat“ tj. zabezpečit dostupnost generických služeb, které souvisejí např. se zabezpečením (PKI, autentizace atd.), mikroplatby, monitoring, sdílení obsahu – syndikaci, transakční návaznosti systémů atd.
- Lze aplikovat individuální přístup v oblasti financování – placená služba i provoz zdarma (např. pro neziskové, dobročinné organizace, školy atd.).
- Dalším argumentem pro poskytování prostředků tímto způsobem na regionální – krajské úrovni je skutečnost jejich „garantovanosti“ tj. lepší kontroly před zneužitím – větší důvěryhodnosti oproti jiným (často zdarma) projektům jenž nabízejí obdobné služby často zneužívané pro nelegální šíření obsahu v konfliktu s autorským právem (tzv. warez pro šíření programů, stránky nabízející hudbu nebo video) či etikou (pornografie).
- Lze nabídnout čisté prostředky, jenž jsou nezbytně nutné pro provoz projektů např. pro mládež, v oblasti vzdělávání, podpory el. obchodu atd. – bez tendenčních reklam nebo odkazu na placené služby (často otevírané na pozadí v řadě oken s nepříliš etickým obsahem).
- V neposlední řadě nabídka služeb i prostředků na úrovni kraje motivuje a stimuluje jejich rozvoj a tvorbu obsahu, což s sebou nese podnikatelskou, pracovní příležitost a rozvoj znalostí v používání prostředků ICT opět na regionální úrovni – v kraji Vysočina.

7.1. Serverhosting

Jako nadstavbovou službu nad vybudováním páteřní sítě a poskytnutím konektivity je serverhosting jakožto připojení serveru (tj. počítače poskytujícího služby) na páteřní síť ISP. Za dodávku služby je potom možné považovat:

- dodávku IP konektivity do síťového rozhraní příslušného počítače,
- dodávku elektrického proudu,
- dodávku provozních prostor (objektů)
- monitoring a správa serverů (na úrovni ICMP (ping), HTTP či fyzicky osobou).

7.2. Webhosting

Dalším možným krokem k poskytování serverhostingu je služba označovaná jako webhosting. Zahrnuje možnost:

- uložení vlastních stránek na vyhrazeném serveru, který je vlastněn a spravován ISP (viz serverhosting). V principu tak ISP prodává prostor na discích svých počítačů, na kterých běží WWW server,
- u dynamického obsahu poskytnutí a sdílení databázového úložiště, jeho lepší škálování a správu chodu,
- sdílení provozních podpůrných služeb – administrace, monitoring, zálohování a archivace,
- vytvoření a provoz garantovaných infrastrukturálních služeb – pro realizaci e-obchodu, podatelny, autentizačních služby, transakční vrstvy atd.

7.3. Outsourcing

Kde to bude pro uživatele výhodné, může část svých potřeb outsourcovat. Připojení na ROWANet umožní místním komerčním subjektům nabízet své služby, jak občanům, tak firmám i organizacím veřejné správy. Technologie VPN umožní, aby například firma využíval on-line služeb účetní firmy v sousedním městě, která zase využívá centrálních serverů pro vedení skladového hospodářství všech firem, kterým vede účetnictví.

Lze si představit dohody v mikroregionech o provozování jednoho společného portálu, a to znova v různých režimech, jak to bude vyhovovat připojeným subjektům (od jednoho portálu se společným obsahem až po několik naprosto nezávislých portálů provozovaných na jednom serveru s jedním správcem).

Většina subjektů může outsourcovat část svých potřeb, například správu firewallů nebo síťových prvků, ale zvláště malé subjekty se mohou spolehnout na centrálně poskytované služby a outsourcovat všechny části svého informačního systému.

8. ROWANet z pohledu uživatele

V předchozích kapitolách byla popsána struktura služeb ROWANetu, postupně popsána podle OSI modelu. V této kapitole se pokusíme popsat několik možností využití takto vybudované infrastruktury. Některé z těchto možností nevyžadují další investice, některé mohou vzniknout až po několika letech provozu.

8.1. Uživatelé ROWANetu

Služeb ROWANetu může využívat celá řada jednotlivců a organizací, ať už ke komunikaci uvnitř organizace, nebo s dalšími organizacemi a jednotlivci. Dle svého zaměření budou využívat jiné služby, je dosti možné, že každý jednotlivý uživatel sítě bude vystupovat v průběhu dne v několika, někdy i v protichůdných rolích (např. zaměstnanec KÚ v roli úředníka a v roli občana, obyvatele obce). Následující výčet možných uživatelů ROWANetu není jistě úplný, spíše se snaží ilustrovat šíři záběru. V podstatě jsou potencionálními uživateli ROWANetu všichni občané kraje Vysočina i všechny organizace působící na jeho území.

- Úřady
 - Krajský úřad
 - Městské a obecní úřady
 - Správa silnic
 - Hasiči
- Firmy
 - Ubytování a rekreace
 - Dopravní podniky
 - Stavební firmy
 - Účetní firmy
 - Banky a spořitelny
- Občané
 - Domácnosti
 - Místní obyvatelé
 - Chataři
 - Příležitostní rekreanti, návštěvníci
- Školy
 - Základní, střední
 - Učitelé a zaměstnanci
 - Žáci a studenti
 - Knihovny a kulturní střediska
- Hrady a zámky
- Informační kiosky
- ...

8.2. Propojovací síť

Základní službou, kterou budou využívat všichni uživatelé připojení do ROWANetu je připojení k Internetu. Lze říci, že i kdyby ROWANet neposkytoval žádnou další přidanou hodnotu, bude tato služba pro rozvoj regionu výrazným přínosem.

Navrhovaná komunikační infrastruktura dovoluje přivést do lokality různé samostatné sítě jednou společnou přípojkou. Technologie postavená na MPLS VPN dovoluje bezpečné oddělení komunikace, takže přes stejné „dráty“, ve stejnou dobu může z jedné školy komunikovat jak učitel, který bude na serveru školní správy vyplňovat vysvědčení, tak i jeho žák, hrající síťovou verzi nějaké počítačové hry se studenty gymnázia ze sousedního města. Při správně navrženém a implementovaném propojení jeden o druhém nebude ani vědět, každý bude komunikovat pomocí své VPN.

Dále může být v rámci ROWANetu postavena celá řada nezávislých propojovacích sítí různých profesních a zájmových organizací. Lze si představit VPN, pomocí které budou komunikovat všechny hasičské sbory kraje nezávisle na ostatním provozu, přes centrální prvky mohou sdílet informace se záchranáři i policií.

Nezávisle na ostatních mohou IP konektivitu využívat všechny možné systémy včasné výstrahy, protipovodňové sondy, zabezpečovací systémy budov, požární čidla.

8.3. Zdroj informací

Síť ROWANet může sloužit jako prostředek pro předávání a pro vyhledávání informací. Od informací na elektronické vývěsce obecního úřadu, přes videozáznamy zasedání krajského zastupitelství až po vyhledání nejvýhodnější nabídky na výkopové práce.

V ROWANetu lze pomocí adresářových služeb publikovat seznamy úředníků, územní rozhodnutí včetně grafického zobrazení v systémech GIS. Na speciálních stránkách je možno publikovat aktuální stav zatopených území při povodních, modely dalšího vývoje, pomocí ROWANetu lze předat i včasné varování připojeným subjektům spolu s pokyny pro evakuaci.

Lze si představit, že na svých webových stránkách, případně na svých portálech budou jednotlivé instituce realizovat značnou část komunikace s občany. Při použití PKI tato komunikace může být oboustranná, mnoha občanům může elektronický podpis při implementaci elektronické podatelny značně zjednodušit život. To se týká jak zaměstnaných lidí, kteří přes den nemají čas k vyřízení komunikace s úřady, tak i pro občany, bydlící v oblastech se špatnou dopravní obslužností.

ROWANet může pomáhat občanům k vyřizování téměř veškeré agendy s úřady, od placení poplatků za psy, přes nahlašování nebezpečných látek, až po zpětnou vazbu úřadům, například formou hlasování o otázkách místní samosprávy.

8.4. Data, Voice, Video

Jeden z výrazných trendů posledních let je tzv. konvergence služeb. Při dostatečně širokém pásmu je systémem jedno, zda přenášené nuly a jedničky jsou ve skutečnosti elektronickou zprávou, telefonním rozhovorem nebo přenos obrazu z přednášky v univerzitní aule. IP telefonie, telekonference, videokonference, webové kamery – jsou technologie, které je možno využívat i na Internetu. ROWANet může nabízet podobné služby s vyšší přidanou hodnotou, protože správce ROWANetu může nastavit QoS (quality of service).

8.5. Bezpečnost sítě

Bezpečnosti jsme se věnovali v předchozích kapitolách. Zde jen zopakujeme, že ROWANet bude nabízet daleko bezpečnější prostředí pro komunikaci, než je klasický Internet. To bude zaručeno jednak použitím centrálních bezpečnostních prvků, jednak možností uživatelů outsourcovat správu své bezpečnosti.

8.6. Zdroj obživy

Infrastruktura sítě ROWANet umožňuje, aby v budoucnu byly vybudovány systémy nabízející služby pro komunikaci dvou komerčních subjektů B2B, tak i pro nabízení služeb zákazníkům B2C.

Systém umožní nabízet služby obyvatelům, například vzdálené vedení účetnictví, skladové hospodářství, vyplňování celních deklarací...

Služby návštěvníkům, zobrazování cyklotras, aktuální situace na silnicích, zobrazení cesty pro vozíčkáře, objednání odvozu – sběr požadavků na odvoz do krajského města a zpětné publikování trasy „pružných“ autobusových linek.

Homeworking/teleworking. Práce doma a práce v centrech pro teleworking může v podstatné míře zvýšit nabídku pracovních míst.

9. Navrhovaný postup prací

V první fázi navrhujeme soustředit se na dobudování infrastruktury na úrovni fyzické vrstvy. Z důvodů nižší ceny je možné v prvních částech první etapy použít technologii VLAN s tím, že při dalším růstu rozsahu ROWANETu dojde k přechodu na MPLS alespoň na úrovni páteře. Pro řešení distribuční a případně přístupové vrstvy je možné technologii VLAN používat i nadále, dokud nebude třeba používat redundantních přenosových tras.

Přitom je rozumné mít na mysli ochranu investic – infrastrukturu budovat na aktivních síťových prvcích, které umožní přejít od infrastruktury na VLAN na infrastrukturu vybudovanou nad MPLS.

Ve druhé fázi je pak třeba doplňovat infrastrukturu redundantními přenosovými trasami a redundantními síťovými prvky tak, aby byla v optimální míře zajištěna dostupnost služeb ROWANETu i při výpadcích a odstávkách. To znamená budovat záložní spoje, doplňovat optická vlákna do topologie do kruhu, uzavírat smlouvy o pronájmu záložní infrastruktury u dalších poskytovatelů spojení atd.

Na úrovni služeb sítě je doporučeno zajistit nutné minimum služeb potřebných k zajištění provozu ROWANETu, tj. DNS, případně NTP a samozřejmě také služby provozního rázu jako je dohled, servis, HelpLine.

Další služby sítě doporučujeme budovat a nabízet ve spolupráci s komerčními subjekty v regionu všude tam, kde je to možné a účelné použít distribuované řešení, pokud možno s několika nezávislými poskytovateli. Při tom je možné používat i partnerství veřejné správy a soukromého sektoru, či různých regionálních sdružení a seskupení společně zajišťující tyto služby. I samotný KÚ může sehrát významnou roli v takových sdruženích.

Není doporučeno budovat veškeré služby sítě a další služby centrálně na úrovni kraje.

Za velkou podporu pro rozvoj regionu lze považovat poskytování přístupu k Internetu v jednotlivých přípojných bodech a to s možností různých úrovní bezpečnosti a přidáných služeb pro připojení k internetu.

Za bezpečnost jednotlivých připojených subjektů musí odpovídat subjekty sami. Ochranu pomocí firewallů, antivirovou ochranu, IDS si každý subjekt musí vybudovat buď sám, nebo si sám musí zvolit nějakou dostupnou službu zpřístupněnou pomocí ROWANETu. Lze samozřejmě spojit investiční prostředky a pomocí metodického vedení (například poskytnutím dokumentace typizované přípojky) snížit náklady na vybudování takových služeb, nebo je možné stimulovat rozvoj obchodních aktivit v této oblasti poskytováním úlev či zajištěním podílového financování pro rozvojové fáze takových aktivit.

To umožní také násobit efekt pro rozvoj kraje a jeho částí. Budou vznikat služby a příležitosti pro podnikatele a zároveň vznikne také nabídka služeb pro veřejnou správu, ze které si bude moci veřejná správa vybírat a nebude závislá jen na jediném poskytovateli všech služeb.

Doporučujeme, aby poskytovatel ROWANETu začal okamžitě budovat infrastrukturu pro dohled a správu sítě včetně podpory uživatelů, jakmile mu to finanční prostředky dovolí. Souběžně s tím navrhujeme investovat do vybudování systému IDS, který lze pro tyto potřeby považovat za bezpečnostní dohled sítě. Vybudování dohledu navrhujeme řešit odděleným projektem.

Bezpečnostní prvky, nabízející služby připojeným subjektům navrhujeme budovat analogicky jako služby sítě tedy jako distribuovanou službu poskytovanou různými subjekty, různými poskytovateli. Nedoporučujeme budovat centrální bezpečnostní prvky jako jediné centralizované řešení a to jak z bezpečnostních, tak organizačních důvodů. Případné sdílené bezpečnostní prvky zajišťované pro potřeby KÚ mohou být poskytovány jako služba jiným organizacím VS v kraji, ale pouze na úrovni dobrovolnosti a s možností volby jiného řešení zajištění bezpečnosti příslušné organizace např. vlastními prostředky či prostředky zajišťovanými jinými subjekty. Proto doporučujeme, aby ROWANET počítal s dalšími subjekty, které budou takové služby poskytovat.

Proto je také rozumné použít co nejdříve technologii IP MPLS alespoň na páteři (případně v kombinaci s VLAN), která umožní propojování VLAN na 3. vrstvě i v jiných lokalitách než v centru a bude umožňovat flexibilnější topologii těchto propojení.

Webhosting, serverhosting jsou služby, které již teď mohou nabízet připojené subjekty i pomocí technologie VLAN. Bezpečnost a flexibilita je však omezena touto technologií.

Po zavedení technologie IP MPLS se situace podstatně zlepší. Poskytovatelé Webhostingu nebo serverhostingu budou moci využívat flexibility VPN poskytovaných RAWANETem k řešení bezpečnosti ve velmi flexibilních podmínkách. To umožní zavádění i dalších služeb s vyššími nároky na oddělení VPN jako je outsourcing jednotlivých služeb i outsourcing aplikací.

10. Přílohy

10.1. e-Europe

Program eEurope je programem EU, který zahrnuje vzájemně se podporující cíle informační společnosti včetně fungování e-governmentu samého, ale také ostatních oblastí praktického života spojeného s informatikou.

Program je všeobecně znám a členské státy EU jej respektují. Na program navazují kritéria hodnocení skutečného stavu v jednotlivých zemích a pravidelné měření stavu a zveřejňování výsledků.

ČR není tak velká a tak ekonomicky ani politicky silná, aby zavedla vlastní kritéria v ostatních zemích EU. To platí i o jednom kraji. Používání vlastních kritérií jen v ČR nebo jen v jednom kraji by vedlo k nečitelnosti a neporovnatelnosti s jinými státy EU, což je vlastně **ekvivalentní s umístěním na posledním místě** ve standardních (ostatními uznávaných) měřeních.

Akční plán „eEurope 2005: An information society for all“ je založen na vzájemně provázaných oblastech:

- Moderní on-line veřejné služby:
 - e-government
 - e-learning services
 - e-health services
- Dynamické prostředí pro e-bussiness

A jako podmiňující pro výše uvedené:

- Široce přístupný širokopásmový přístup za konkurenceschopné ceny
- Bezpečná informační infrastruktura

Program eEurope 2005 je určen i pro nově přistupující země a tedy i pro ČR.

Nadprůměrné výsledky v programu informatizace EU (eEurope) znamenají lepší podmínky pro podnikání (zejména pro podnikání spojené se znalostní ekonomikou) než jsou průměrné a lepší podmínky k životu než jsou průměrné v celé EU. A to zejména dostupnější, rychlejší a levnější služby VS pro podnikatele. Vytvoření transparentního prostředí pro podnikatele, automatizace a zrychlení některých služeb veřejné správy sníží rizika korupce a vytvoří lepší podmínky pro veřejnou kontrolu. To vše vytváří konkurenční výhodu pro podnikatele v případě, že bude podnikat na území ČR, na území kraje. To by měl být stimul pro umístování podnikatelských aktivit na vybraném území ČR a tím posílit ekonomiku kraje (tedy jak příjmy veřejných rozpočtů, tak vyšší nabídku pracovních příležitostí a tedy i vyšší příjmy obyvatel).

Přestože se tento cíl může na první pohled zdát jako těžko dosažitelný nebo dokonce přemrštěně ambiciózní, je to de facto minimální cíl s ohledem potřeby, na realitu světa a na podmínky ČR a kraje (historická úroveň vzdělání a kultury, nedostatek přírodních zdrojů, poloha uprostřed Evropy).

V budoucnu ČR ani kraj v rámci EU nemůže stavět svoji další prosperitu na nižších cenách pracovní síly. To by vedlo k systematickému zaostávání životní úrovně. Musí hledat jinou komparativní výhodu. Lepší prostředí pro podnikání i pro život takovou výhodou může být.

Primárním cílem e-governmentu je zrychlit a zproduktivnit služby VS pro obyvatele, pro firmy, pro zprostředkovatele (agenty). Efektem e-governmentu je zvýšení produktivity ve VS, snížení nároků na objem prací úředníků a zvýšení nároků na kvalifikaci, odpovědnost a schopnost rozhodovat.

Změna chápání VS – přesun k modernímu demokratickému pojetí VS uplatňovaném ve vyspělých státech EU – VS je veřejná služba občanům usnadňující jejich soužití (a ne nástroj moci a nátlaků na občany).

Úspěch informatizace umožní firmám flexibilnější a efektivnější fungování oproti zemím s nižší úrovní informatizace. To umožní rychleji a efektivněji využívat nových šancí na trhu, obsazování nových trhů a lepší přizpůsobení se požadavkům zákazníků.

Informatizace a znalostní ekonomika má potenciál podstatně pomoci v regionálním rozvoji zejména v problematických regionech. Využíváním moderních technologií vzdálené komunikace má šanci minimalizovat vliv skutečné lokality a tedy podstatně zmírnit či úplně smazat rozdíl mezi působením ve vyspělém regionu či na venkově nebo v regionu s nedostatkem pracovních příležitostí.

Zprostředkovatelské firmy (agenti) budou fungovat efektivněji a budou moci nabízet své specializované služby levněji a v širší nabídce oproti současnosti. Širší používání služeb zprostředkovatelů zlepší podmínky i pro VS, protože část osvětové práce a přípravy kvalitních pokladů budou dělat kvalifikovaní lidé se zkušenostmi.

Občanům umožní pohodlnější život a lepší spolupráci s VS.

Při vysokém stupni využívání e-governmentu se podstatně změní poměry objemů prací ve VS. Podstatně se sníží nároky na objem prací „přepážkových pracovníků“, tedy na jejich počet. Zvýší se ale nároky na kvalifikaci a kvalitu práce úředníků, kteří budou ve VS rozhodovat, zejména na rychlost rozhodnutí a sníží se pracnost s tím spojená.

S úspěchem informatizace je spojen i rozvoj trhu služeb ICT. Zvýší se potřeba firem i VS využívat kvalitních služeb ICT a zároveň se zvýší tlak na jejich kvalitu, dostupnost a spolehlivost. S dalším rozvojem technologií se bude stále zvyšovat náročnost na úroveň know-how a tím i prohlubující se nedostatek kvalifikovaných odborníků. To povede pravděpodobně k vyšší profesionalizaci těchto služeb, tedy k hromadnějšímu poskytování služeb ICT, vyšší úrovni dělby práce uvnitř firem poskytujících služby ICT, vyšší úrovni většímu rozsahu služeb poskytovaných „na klíč“ a to jak pro komerční sféru, tak pro VS.

To povede ke zdražování těch nejkvalifikovanějších služeb ICT a dalšímu prohlubování propasti (znalostí, zkušeností, pracovních návyků a pravděpodobně i platů) mezi ICT technickými specialisty VS a komerční sférou.

Budou i další negativní dopady. Je možné očekávat zejména nové formy kriminality spojené s informatizací. Těm nebude možné čelit bez kvalifikovaných expertů a řádného vybavení VS a to nejen kriminalistů. Např. jedním z kritických oblastí bude rychlost reakce VS při aplikaci protipatření při ohrožení nějakou zatím neznámou formou elektronické kriminality či terorismu.

10.1.1. Quick win

Pojmem „Quick win“ je často pojmenovávána efektivní strategie rozhodování v prostředí rychle se měnícího světa s obrovským množstvím těžko postižitelných vazeb, týkajících se velkého počtu lidí. Pro využívání ICT ve VS je charakteristické následující:

- Technologie ICT mají velmi krátký inovační cyklus.
- Velmi rychle se mění názory lidí na možnosti jejich využívání, na to co je a co není moderní, užitečné, vhodné.
- Všechny osoby, kterých se konkrétní projekt týká, není možné věrohodně zapojit do detailních rozhodovacích procesů a to i proto, že jim nelze věrohodně ukázat podstatu věci, dokud něco doopravdy nefunguje.

Proto je tato strategie rozhodování založena na výběru cíle, který je reálně dosažitelný s disponibilními prostředky (lidskými, technologickými, finančními), který je dosažitelný velmi rychle (řádově týdny až měsíce, výjimečně roky), a který má maximální praktické pozitivní výsledky. Tedy **pečlivé hledání a výběr nejsnáze dosažitelného cíle a jeho opravdové dosažení**.

Další cíl je specifikován až v době, kdy je to nutné a možné (např. až po dosažení cíle předchozího). V té době jsou známy přínosy předchozího (ty maximální dobré) a tedy je mnohem pozitivnější prostředí pro stanovení náročnějšího cíle. Zároveň je znám nový stav technologií a také reakce lidí na předchozí etapu. Tedy stanovení dalšího cíle bude mnohem přesnější než pokud by k tomu došlo dříve. A tedy šance na úspěch dalšího cíle je větší.

Tato strategie rozhodování nemusí být v rozporu s nějakou dlouhodobou koncepcí či dlouhodobou strategií. Shoda konkrétního vybíraného cíle s takovou dlouhodobější koncepcí může být jedním z pomocných výběrových kritérií a zároveň výběr konkrétního cíle je ověřením kvality a správnosti takové dlouhodobé strategie.

10.1.2. Výběr cílů

Příprava cíle je nejdůležitější etapou která nejvíce ovlivňuje konečný úspěch i celkové náklady. Je rozumné věnovat na přípravu cíle cca 5-20% celkových nákladů na řešení. Účelně vynaložené náklady na přípravu cíle bývají neefektivněji investované prostředky s nejvyšším pozitivním efektem. Mohou přinést mnohonásobný efekt již při realizaci a další mnohonásobné efekty v době využívání.

Zejména pro ty nejdůležitější programy a projekty se vyplatí alternativní nezávislý výběr a příprava cíle, i když se to na první pohled bude zdát jako plýtvání či vyhození prostředků za nepřijatou variantu. To ale není pravda. To souvisí s cenou kvalitní informace.

Alternativní výběr cílů má efekt nejen ve vzniku více variant s různými vlastnostmi ze kterých je možno vybírat, ale také v tom, že všichni autoři nemají monopolní postavení a jsou stimulováni k vyšší kvalitě té své varianty. Obojí má podstatný pozitivní vliv na kvalitu informací, které jsou použity k přípravě cíle. A kvalita informací podstatně ovlivňuje kvalitu rozhodování a následně i kvalitu celého díla.

10.1.3. Systém měření a vyhodnocování

Podstatnou vlastností rozvoje ICT je měřitelnost výsledků. To znamená, že cíl je kvantitativně měřitelný a je možno jasně vidět, zda jej bylo dosaženo a kdy. To je strategie v praxi uplatňovaná v EU.

Měření výsledků je prováděno pravidelně a z něj je patrné, jaký pokrok byl dosažen mezi měřeními, jaká vzdálenost chybí k cíli a kde je situace lepší a kde horší. To samozřejmě pomůže se soustředit na to co je opravdu potřeba a pomůže lépe využít omezených disponibilních zdrojů.

EU věnovala stanovení měřitelných kritérií a všemu co s tím souvisí značné úsilí, prostředků a času. Do tohoto procesu bylo zapojeno řada institucí, firem a odborníků a také mnoholetých praktických zkušeností z řady zemí. Způsoby vyhodnocování jsou a budou i nadále zlepšovány a přizpůsobovány měnícímu se světu (např. inovace indikátorů EU na konci roku 2002).

Nový vývoj analogických kritérií jen pro ČR, nebo dokonce jen pro jeden region by byl zbytečným plýtváním omezených prostředků. Naopak ČR má možnost využít toho co je hotové a ověřené stejně jako ostatní země EU a může své omezené zdroje soustředit na jiné oblasti.

Pokrok informatizace v kandidátských zemích (eEurope+ 2003), ke kterému se již ČR oficiálně přihlásila, je již dnes měřen stejnými kritérii (pokud jsou k dispozici potřebné podklady) jako v členských státech EU a výsledky jsou porovnávány s výsledky z členských států.

Měřitelnost cílů pomáhá řešit i velmi obtížnou úlohu výběru programů a projektů, které budou realizovány a pomáhá k zamítnutí těch méně efektivních, tedy k soustředění zdrojů (finančních, lidských, organizačních, času,). To povede k dosažení těch nejvyšších efektů v měřitelných kritériích a následné měření v průběhu realizace a po ní ukáže opravdový dosažený pokrok a tedy umožní objektivně zhodnotit efektivitu vynaložených zdrojů.

10.1.4. Kriteria měření eEurope 2002

Program eEurope je měřen pomocí 23 klíčových indikátorů v 11 oblastech odsouhlasených v listopadu 2000.

Jedná se o:

Levnější, rychlejší internet

1. Procento populace pravidelně používající internet.
2. Procento členů domácností s přístupem k internetu z domova.
3. Cena přístupu k internetu.

Rychlejší internet pro výzkumníky a studenty

4. Rychlost propojení a služby uvnitř a mezi národními vzdělávacími a výzkumnými sítěmi (NRENs) v rámci EU a celosvětově.

Bezpečné sítě a smartkarty

5. Počet zabezpečených serverů na milion obyvatel.
6. Počet uživatelů internetu se zkušeností s bezpečnostními problémy.

Evropská mládež v digitálním věku

7. Počet počítačů na 100 žáků v primární/sekundární/terciální úrovni.
8. Počet počítačů připojených na internet na 100 žáků v primární/sekundární/terciální úrovni.
9. Počet počítačů s vysokorychlostním připojením na internet na 100 žáků v primární/sekundární/terciální úrovni.
10. Procento učitelů používajících internet pro pravidelnou výuku v nepočítačových oborech.

Práce ve znalostní ekonomice

11. Procento pracovní síly s (alespoň) základními IT dovednostmi.
12. Počet pracovních míst a absolventů ICT odpovídajících třetí úrovni vzdělání.
13. Procento pracovní síly používající „telework“ (práci ze vzdálené lokality pomocí telekomunikačních technologií).
14. Účast pro všechny ve znalostní ekonomice.
15. Počet míst s veřejně přístupným internetem (PIAP) na 1000 obyvatel.
16. Procento webů centrálních vládních institucí (central government websites), které vyhovují WAI (Web Accessibility Initiative) úrovni A.
17. Akcelerace e-commerce.
18. Procento firem, které nakupují a prodávají přes internet.
19. Veřejná správa on-line.
20. Procento základních veřejných služeb přístupných on-line.
21. Veřejné využívání on-line služeb veřejné správy – pro informaci / pro zasílání formulářů.
22. Procento veřejných zakázek, které mohou být provedeny on-line.
23. Zdraví on-line.
24. Procento zdravotníků s přístupem k internetu.
25. Užití různých kategorií obsahu webu zdravotníky.
26. Evropský digitální obsah (digital content) pro globální síť.
27. Procento webů EU v národních žebříčcích 50 nejnavštěvovanějších.
28. Inteligentní dopravní systémy.
29. Procento dálniční sítě (k celkové délce sítě) vybavené informačním a řídicím systémem pro případ zahlcení (dopravní zácpy).

10.1.5. Kriteria měření služeb e-governmentu

Věřené služby e-governmentu jsou testovány ve 12 službách určených pro (individuální) občany a 8 službách pro podniky.

Jsou to – pro občany:

1. Příjmové daně
2. Hledání zaměstnání
3. Sociální zabezpečení
4. Osobní doklady
5. Registrace motorových vozidel
6. Žádosti ke stavebnímu povolení
7. Oznámení pro policii
8. Veřejné knihovny
9. Rodné listy a oddací listy
10. Přihlášení (zápis) na vyšší školy
11. Oznámení o stěhování
12. Služby spojené se zdravotnictvím

Pro firmy:

1. Sociální příspěvek pro zaměstnance
2. Podnikové daně
3. Daně s přidané hodnoty (DPH)
4. Registrace nové firmy
5. Podání statistických dat
6. Celní deklarace
7. Povolení spojená s ochranou životního prostředí
8. Veřejné zakázky

V těchto službách jsou definovány 4 základní fáze či etapy a to:

Etapa1 – **informace** – on-line informace o veřejných službách.

Etapa2 – **interakce** – elektronické stažení formulářů.

Etapa3 – **dvousměrná interakce** – zpracování formulářů včetně autentizace.

Etapa4 – **transakce** – vyřízení případu; rozhodnutí a doručení (platba).

Z výsledků měření v EU je patrné, že vlády členských zemí velmi často upřednostňují služby pro firmy a to služby nejvyšší kvality (transakce). To má své racionální důvody, neboť firmy pomáhají rozvíjet ICT svými investicemi jak do znalostí, tak do vybavení a nabídky elektronických služeb pro ostatní firmy a pro veřejnost.

Má to své racionální důvody i pro veřejnou správu, protože počet transakcí veřejné správy na jednu firmu je mnohonásobně vyšší než na jednoho občana a tedy automatizace takových transakcí přináší vyšší efekty také pro veřejnou správu a investice veřejné správy do této oblasti jsou efektivnější.

Z toho vyplývá, že je racionální upřednostnit v ČR zejména rozvoj služeb VS pro firmy a tedy zejména transakční elektronické služby:

- Sociální příspěvek pro zaměstnance
- Podnikové daně
- Daně s přidané hodnoty (DPH)
- Registrace nové firmy
- Podání statistických dat
- Celní deklarace
- Povolení spojená s ochranou životního prostředí
- Veřejné zakázky

Protože služby pro občany jsou také důležité, je rozumné rozvíjet tyto služby a to zejména ty, kde je to málo náročné na zdroje a kde je možné dosáhnout velkých efektů pro občany i pro veřejnou správu. Jedná se zejména o tyto služby:

- Příjmové daně
- Hledání zaměstnání
- Sociální zabezpečení
- Osobní doklady
- Registrace motorových vozidel
- Žádosti ke stavebnímu povolení
- Oznámení pro policii
- Veřejné knihovny
- Rodné listy a oddací listy
- Přihlášení (zápis) na vyšší školy
- Oznámení o stěhování
- Služby spojené se zdravotnictvím

A i v této oblasti je rozumné podporovat vysoké úrovně elektronických služeb. Nemusí však být rozumné uměle zavádět transakce, vzhledem k problematice hromadné elektronické autorizace a to do doby běžnějšího používání elektronické autorizace v normálním životě (např. v elektronickém obchodě). Pro první období je pravděpodobně rozumnější podporovat především takové způsoby elektronické interakce VS s občany, které nebudou občany příliš zatěžovat a to i za cenu, že nebudou zcela ideální z pohledu odborníků z oboru informatiky, tedy např. vhodnou formu obousměrné komunikace. Důležitější je širší spektrum elektronických služeb poskytovaných VS pro občany než informaticky perfektní osamocená služba.

10.1.6. Kriteria měření eEurope 2005

V souvislosti s inovovaným programem EU eEurope 2005 byly v listopadu 2002 inovovány indikátory EU pro měření a to i s ohledem na nové členy EU. Jedná se o 10 skupin se 14 zásadními indikátory a 22 doplňkovými indikátory (a 1 zásadním a 3 doplňkovými, které budou pilotně ověřovány).

Omezený počet zásadních indikátorů, které jsou snadno srozumitelné, má za cíl dát podklady k zásadním politickým rozhodnutím. Doplňkové statistické indikátory jsou určeny jako data pro analýzy a pro porovnávání s dalšími zeměmi mimo EU.

Je určeno také časování vyhodnocení (data musí být k dispozici v listopadu) a také návaznosti na standardní procesy EU (např. na Eurostat a národní statistiky).

Je počítáno se zapojením kandidátských zemí od roku 2003.

Jedná se o tyto skupiny a jednotlivé identifikátory:

Internetové identifikátory

A. Přístup obyvatel na internet

Zásadní indikátory:

A.1 - procento členů domácností nebo fyzických osob, které mají přístup k internetu z domova.

A.2 - procento fyzických osob pravidelně používajících internet.

Zdroj: Eurostat/ NSI ICT průzkum domácností (data budou sbírána na porovnatelné bázi).

Frekvence vyhodnocení: 1x ročně v říjnu.

První vyhodnocení – říjen 2003

Doplňkové statistické indikátory:

A.3 – procento členů domácností s přístupem k internetu podle typu přístupového zařízení (digitální TV, mobilní,...).

A.4 – procento fyzických osob s přístupem k internetu podle místa přístupu (domácnost, zaměstnání, škola, veřejná místa,...).

A.5 – procento fyzických osob s přístupem k internetu podle specifického účelu použití internetu (přijímání/odesílání elektronické pošty, hledání informací, hraní her, internetové bankovníctví,...).

A.6 - procento členů domácnosti připojených v oblastech „Objective 1“.

B. Přístup firem a využívání ICT firmami

Zásadní indikátor:

B.1 – procento zaměstnanců používající počítač připojený k internetu ke své normální práci

Zdroj: Eurostat/ NSI ICT průzkum firem

Frekvence vyhodnocení: 1x ročně v říjnu.

První vyhodnocení – říjen 2003

Doplňkové statistické indikátory:

B.2 - procento firem majících přístup na internet

B.3 – procento firem majících webové stránky

B.4 – procento firem používajících intranet/extranet

B.5 – procento firem se zaměstnanci, pracujícími alespoň část pracovní doby mimo firmu a používající vzdáleně informační systém firmy

C. Cena přístupu k internetuZásadní indikátor:

C.1 – cena přístupu k internetu podle frekvence použití (20, 30, 40 hodin/měsíc, neomezeně)

Zdroj: Studie komise + OECD

Frekvence vyhodnocení: 1x ročně v říjnu.

První vyhodnocení – říjen 2003

Doplňkový statistický indikátor:

C.2 – specifikace nejlevnějšího širokopásmového přístupu k internetu podle typu přístupu v každém členském státě

Moderní on-line služby**D. e-government**Zásadní indikátor:

D.1 – počet základních veřejných služeb plně přístupných on-line

Frekvence vyhodnocení: 1x ročně v říjnu.

Zdroj: Studie komise ve spolupráci s členskými státy

První vyhodnocení – říjen 2003

Doplňkové statistické indikátory:

D.2 – procento fyzických osob používajících internet ke kontaktu s veřejnou správou podle účelu (získání informací, získání formulářů, předání formulářů)

D.3 - procento firem používajících internet ke kontaktu s veřejnou správou podle účelu (získání informací, získání formulářů, předání formulářů)

Doplňkové statistické indikátory určené k pilotnímu ověření:

D.4 – počet veřejných služeb plně integrovaných s digitálními vnitřními agendami

D.5 – objem veřejných zakázek plně prováděných on-line (elektronicky integrovaných) v % celkového objemu veřejných zakázek

D.6 – procento veřejných institucí používajících „open source software“

E. e-learningZásadní indikátor:

E.1 – počet žáků na počítač s internetovým připojením (širokopásmově/neširokopásmově).

Zdroj: Studie komise / Eurostat / NSI průzkumy domácností, firem.

Frekvence vyhodnocení: 1x ročně v říjnu.

První vyhodnocení – říjen 2003

Doplňkové statistické indikátory:

E.2 – procento fyzických osob používajících internet ve vztahu ke vzdělávání a zvyšování kvalifikace podle typů vzdělávání (školy, postgraduální studium, další formy).

E.3 – procento firem používajících e-learning ke školení a vzdělávání zaměstnanců.

F. e-healthZásadní indikátor:

F.1 – procento obyvatel (16 let a starších) používajících internet k vyhledávání zdravotních informací pro sebe nebo jiné

F.2 – procento všeobecných praktických lékařů používajících elektronických záznamů o pacientech

Zdroj: Nový průzkum, Eurostat / NSI průzkumy domácností

Frekvence vyhodnocení: 1x ročně v říjnu.

První vyhodnocení – říjen 2003

Dynamické prostředí pro e-bussines**G. nákup a prodej on-line**Zásadní indikátor:

G.1 – procento celkového obrátu firem z e-commerce

Zdroj: Eurostat / NSI průzkumy firem, průzkumy domácností

Frekvence vyhodnocení: 1x ročně v říjnu.

První vyhodnocení – říjen 2003

Doplňkové statistické indikátory:

G.2 – procento fyzických osob nakupujících zboží a nebo služby pro soukromou spotřebu přes internet v posledních 3 měsících

G.3 – procento firem přijímajících on-line objednávky

G.4 – procento firem přijímajících on-line platby při prodeji přes internet

G.5 – procento firem nakupujících on-line

H. e-bussines připravenost

Zásadní indikátor:

e-bussines index (složený indikátor) – bude pilotně ověřováno v roce 2003

Zdroj: Eurostat / NSI průzkumy firem

Pilotní vyhodnocení – říjen 2003, pokud bude akceptovatelné, další vyhodnocování 1x ročně.

Součástí indexu:

Přijetí ICT v obchodě

a1 – procento firem používajících internet

a2 – procento firem majících webové stránky

a3 – procento firem používajících alespoň dva bezpečnostní prostředky v době průzkumu

a4 – procento zaměstnanců používajících počítač k normální práci

a5 – procento firem s širokopásmovým připojením k internetu

a6 – procento firem s LAN a používajících internet nebo extranet

Užití ICT v obchodě

b1 – procento firem které nakupují produkty /služby přes internet nebo jiným elektronickým způsobem v objemu větším než 1% celkového nákupu

b2 – procento firem které přijímají objednávky přes internet nebo jiným elektronickým způsobem v objemu větším než 1% celkového obrátu

b3 – procento firem jejichž informační systém pro objednávky a nákupy je automaticky propojen s vnitřními informačními systémy

b4 – procento firem jejichž informační systémy jsou automaticky propojeny s informačními systémy zákazníků a dodavatelů

b5 – procento firem s internetovým připojením používajících internet pro bankovní a peněžní služby

b6 – procento firem, které prodaly produkty jiným firmám pomocí účasti na specializovaných elektronických tržištích.

Bezpečná informační infrastruktura

I. Zkušenosti a užití internetu s ohledem na bezpečnost ICT

Zásadní indikátory:

I.1 – procento fyzických osob s přístupem k internetu, které se setkaly s bezpečnostními problémy

I.2 - procento firem s přístupem k internetu, které se setkaly s bezpečnostními problémy

Zdroj: Eurostat / NSI průzkumy domácností a firem

Frekvence vyhodnocení: 1x ročně v říjnu.

První vyhodnocení – říjen 2003

Doplňkové statistické indikátory:

I.3 – procento fyzických osob které udělaly ICT bezpečnostní opatření v posledních 3 měsících

I.4 – procento firem které udělaly ICT bezpečnostní opatření v posledních 3 měsících

I.5 – procento fyzických osob a firem, které instalovaly bezpečnostní prostředky na jejich PC a aktualizovaly je v posledních 3 měsících

Širokopásmová komunikace**J. Rozšíření širokopásmové komunikace**Zásadní indikátory:

J.1 – procento firem s širokopásmovým přístupem

J.2 – procento členů domácností nebo fyzických osob s širokopásmovým přístupem

J.3 – procento veřejné správy s širokopásmovým přístupem

Zdroj: Studie komise/ Eurostat / NSI průzkumy domácností a firem

Frekvence vyhodnocení: 1x ročně v říjnu.

První vyhodnocení – říjen 2003

Doplňkové statistické indikátory:

J.4 – rozlišení mezi dostupností a využíváním širokopásmového přístupu k internetu podle typů přístupu

J.5 – procento členů domácnosti nebo fyzických osob s domácím síťovým připojením.

Poznámka:

Tyto indikátory jsou navrženy tak, aby byly porovnatelné s daty z USA, Japonska a ostatními vyspělými státy.

10.1.7. Současná pozice ČR

Podle hodnocení úrovně informatizace v kandidátských zemích, které proběhlo jako součást programu eEurope+ 2003 v červnu 2002 jako podklad ke konferenci ministrů kandidátských zemí o informační společnosti v Lublani **je ČR průměrnou kandidátskou zemí.** Z 18 kvantitativně hodnocených kritérií má ČR v 6 kritériích lepší výsledky než je průměr mezi kandidátskými zeměmi, v 5 kritériích jsou výsledky ČR průměrné nebo těsně podprůměrné a v 6 kritériích jsou horší než je průměr kandidátských zemí (jedno kritérium pravděpodobně nebylo z nějakého důvodu v případě ČR hodnoceno). **Pouze v jediném dílčím kritériu je ČR lepší než je průměr v EU.** Tímto kritériem je cena přístupu na internet v době mimo pracovní dobu přepočtená na kupní sílu. **Ve všech ostatních hodnocených kritériích** (tedy i v ceně přístupu na internet v pracovní době) **je ČR horší než je průměr současných členů EU.**

Kritérium	ČR	Průměr kandidátských zemí	Průměr členských zemí
Procento domácností s pevným telefonem	68 %	77 %	86 %
Počet mobilních telefonů na 100 obyvatel	66	39	75
Počet pevných linek na 100 obyvatel	36	35	55
Procento obyvatel pravidelně používající Internet	28 %	17 %	47 %
Procento domácností s přístupem na Internet	10 %	10 %	38 %
Cena přístupu na Internet (přepočteno na standardní kupní sílu) – ve špičce	3.9 Euro/hod	3.1 Euro/hod	1.7 Euro/hod
Cena přístupu na Internet (přepočteno na standardní kupní sílu) – mimo špičku	1.0 Euro/hod	1.7 Euro/hod	1.7 Euro/hod
Poměrná doba špičky na 1 hod.	18min	17 min	-
Počet PC na 100 obyvatel	12	13	33
Počet uživatelů Internetu na 100 obyvatel	13	14	32
Počet míst s veřejným přístupem k Internetu na 1000 obyvatel	0.1	0.18	-
Počet internetových hostů (připojených počítačů) na 100 obyvatel	2.1	1.3	5.4
Počet PC na 100 žáků v primární úrovni vzdělávání (základní školy)	3.9	4.0	11.1
Počet PC připojených k Internetu (na 100 žáků základních škol)	1.9	2.2	5.0
Počet PC připojených k vysokorychlostnímu Internetu (na 100 žáků základních škol)	-	1.0	-
Počet PC na 100 studentů v sekundární úrovni vzdělávání (střední školy)	5.9	4.3	15.4
Počet PC připojených k Internetu (na 100 studentů středních škol)	3.2	2.7	10.8
Počet PC připojených k vysokorychlostnímu Internetu (na 100 studentů středních škol)	-	0.8	-
Počet PC na 100 studentů v terciálních školách (vysoké školy)	-	5.0	25.2
Počet PC připojených k Internetu (na 100 studentů vysokých škol)	-	3.8	16.7
Počet PC připojených k vysokorychlostnímu Internetu (na 100 studentů vysokých škol)	-	2.7	-

Poznámka:

Údaje ČR týkající se školství jsou z roku 2000. Údaje které nebyly v citovaném porovnání [34] uvedeny jsou označeny -.

Ostatní kritéria obsažená v hodnocení jsou vyhodnocena globálně a charakterizují situaci v kandidátských zemích jako celku a nelze z nich vyčíst postavení ČR ani s ohledem na průměr kandidátských zemí, ani s ohledem na situaci v EU.

Ze závěrů vyplývá, že situace v kandidátských zemích je značně rozdílná. Některé kandidátské země jsou na tom lépe než mnoho členů EU. To se týká zejména Malty, Kypru a Slovinska.

11. Literatura

Obsahuje odkazy na nejdůležitější informační zdroje použité jako podklady při zpracování tohoto textu.

- [4] Program eEurope+ 2003 „A co-operative effort to implement the Information Society in Europe“, prepared by the Candidate Countries with assistance of the European Commission, June 2001,
http://europa.eu.int/information_society/topics/international/index_en.htm
- [5] Dokument EU „eEurope 2005: An information society for all“, An Action Plan to be presented in view of the Special European Council, 21/22 June 2002,
http://europa.eu.int/information_society/eeurope/action_plan/index_en.htm
- [6] Dokument EU „eEurope 2002: An information society for all – Action Plan“, prepared by the Council and the European Commission for the Special European Council, 19-20 June 2002,
http://europa.eu.int/information_society/eeurope/action_plan/index_en.htm
- [7] Dokument EU „eEurope - An information society for all“, Communication on an Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000,
http://europa.eu.int/information_society/eeurope/action_plan/index_en.htm
- [8] Web-based Survey on Electronic Public Services „SUMMARY REPORT“, (Results of the first measurement: October 2001), European Commission, DG information society, Cap Gemini Ernst & Young, listopad 2001.
- [9] Výsledky měření výsledků e-europe, Benchmarking E-europe,
http://europa.eu.int/information_society/eeurope/benchmarking/index_en.htm.
- [10] Výsledky měření výsledků e-europe, Benchmarking E-europe, 2002,
http://europa.eu.int/information_society/eeurope/benchmarking/list/2002/index_en.htm).
- [14] ARCHITECTURE GUIDELINES For Trans-European Telematics Networks for Administrations, Version 5.3, Enterprise DG/B/5, Brussels, February 2001.
- [15] PROJECT INTDIR, Contract No 503315, Integration of Directory services in IDA services and applications, FINAL REPORT, verze V.03B, Singular, 12 October 2001.
- [16] TESTA A catalogue of services, Version 1.25, IDA, 5. June 2001.
- [17] Security Requirements Statement for the IDA Communication Platform, Draft 0.3, 14.9. 2001.
- [18] Konceptní návrh řízení komunikační infrastruktury, verze 1.0, ANECT a.s., Brno, 13. prosince 2001.
- [19] Konceptní návrh projektu „adresářové služby“, Compaq, prosinec 2001.
- [20] Centrální podpora uživatelů - Konceptní návrh projektu, KPMG Consulting, 14. prosince 2001.
- [21] Konceptní návrh projektu „infrastruktura veřejného klíče“, IBM, Secunet, prosinec 2001.
- [22] Konceptní návrh pro úvodní etapu řešení projektu Metainformační systém, Aquasoft s.r.o, prosinec 2001.
- [23] Konceptní návrh projektu „Přístupový portál“, ICZ, IBM, prosinec 2001.

- [24] Referenční rozhraní - Koncepční návrh projektu, Deloitte&Touche, 17. prosince 2001.
- [25] Koncepční návrh projektu ZRES pro ÚVIS, Oracle Czech s.r.o., 14. prosince 2001.
- [26] Metodika využívání komunikační infrastruktury veřejné správy, verze 1.00i, ÚVIS, Duben - Říjen 2002.??
- [27] Celková bezpečnostní politika komunikační infrastruktury veřejné správy, verze 1.00, ÚVIS, Březen -Červenec 2002.
- [31] Dokument EU „Key indicator list“, listopad 2000 - http://europa.eu.int/information_society/eeurope/benchmarking/index_en.htm
- [32] Dokument EU „eGovernment indicators for benchmarking eEurope“, únor 2001.
- [33] Dokument EU „eEurope 2005: benchmarking indicators“, listopad 2002 - http://europa.eu.int/information_society/eeurope/news_library/documents/index_en.htm.
- [34] Dokument „eEurope+ 2003 – Progress Report June 2002“ - <http://emcis.gov.si/>.