

Sít'ová bezpečnost

I. Základní popis zabezpečení

1. Úvod

Pojmem bezpečnost rozumíme nikoliv stav, ale neustálý proces, kterým se snažíme dosáhnout a udržet uspokojivé zabezpečení sítě. Sít'ové technologie se velmi rychle vyvíjí a s nimi rovněž také znalosti a nástroje potenciálních útočníků. Potenciální hrozbou pro síť jsou lidé (nedbalost či neznalost uživatelů nebo úmyslné útoky, krádeže apod.) a přírodní faktory (blesk, požár, záplavy apod.). Dříve než začneme plánovat zabezpečení vlastní sítě, je třeba nejdříve zvážit jakou cenu mají aktiva (hardware, software, data) a jaká jsou s jejich případným zneužitím, odcizením či poškozením spojená rizika (ztráta zákazníků, poškození dobrého jména organizace apod.) tak, aby plánované prostředky vynaložené na zabezpečení byly na jednu stranu dostatečné ale nikoliv zase přemrštěné (pro příměr: aby nebyl sejf dražší než jeho obsah). V souvislosti s možným výskytem bezpečnostních incidentů (narušení bezpečnosti) je třeba mít připraven plán jejich zvládnutí (adekvátních reakcí na ně) včetně plánu zachování (či rychlého obnovení) chodu organizace až do jejich úplného vyřešení a návratu do původního stavu. Náplní předchozích dvou souvětí se zabývá zejména:

- risk management ¹
 - identifikace aktiv a stanovení jejich hodnoty
 - identifikace hrozeb a slabin
 - stanovení závažnosti hrozeb a míry zranitelnosti
- disaster recovery plan ²
 - prevence bezpečnostních incidentů
 - detekce bezpečnostních incidentů
 - obnova po výskytu bezpečnostního incidentu
- business continuity management ³
 - porozumění činnosti organizace
 - návrh a implementace bezpečnostních opatření (interní předpisy, bezpečnostní politika, DRP, BCP, strategie reakcí na incidenty)
 - audit, testování, hodnocení a případná změna bezpečnostních opatření
- business continuity plan
 - aktualizované off-site úložiště dat a dokumentů (smlouvy, pojištění, účetnictví)
 - kontakty na zaměstnance, krizové vedení a obchodní partnery
 - směrnice a postupy pro aktivaci disaster recovery plánu
- strategie reakcí na incidenty
 - ochrana životů a zdraví
 - zamezení dalších škod
 - hodnocení škod
 - použití BCP (+ obnova běžného chodu organizace dle DRP)

Kromě toho, že útoky na bezpečnost sítě můžeme dělit dle lokace útočníka na vnitřní (neznalost, nedbalost či útok ze strany vlastních zaměstnanců) a vnější (náhodný či promyšlený útok zvenčí), bezpečnost sítě lze rozdělit na fyzickou bezpečnost, bezpečnost sítě a služeb a bezpečnost lidských

zdrojů.

2. Fyzická bezpečnost

- ✓ vhodná lokalita pro sídlo organizace (či pro umístění jejího IT zázemí)
 - dobrá dopravní dostupnost (optimálně alespoň dvěma způsoby – auto, MHD, vlak, ...)
 - ochrana před nepříznivými přírodními vlivy
 - vyvýšený vchod (kvůli záplavám či závějím)
 - neumísťovat v záplavovém pásmu
 - neumísťovat přímo pod kopec či do svahu (riziko zavalení či sesuvu půdy)
 - neumísťovat příliš blízko stromům (nebezpečí jejich pádu atd.)
- ✓ splnění elektrotechnických předpisů
 - správné dimenzování vodičů a jističů
 - dostatečné uzemnění a izolace
 - správné IP krytí zařízení
 - proudové chrániče
 - ochrana před bleskem a přepětím
- ✓ splnění požárních předpisů ⁴
 - žáruvzdorné materiály
 - správný hasicí systém
 - požární hlásič
 - únikový východ
- ✓ zabezpečení klíčových prostor
 - uzamykatelné prostory, bezpečnostní dveře, bezpečnostní fólie
 - EZS ⁵
 - kamerový dohled, ostraha
 - evidence vstupu povolaných osob (čipové karty, otisk prstu apod.)
 - ochrana budovy (mříže na oknech, plot, betonové zátarasy apod.)
- ✓ zajištění vhodného prostředí pro provoz informační a komunikační techniky
 - spolehlivé dodávky el. energie (UPS ⁶, motorgenerátor, náhradní dodavatel elektrické energie)
 - odvětrávání, chlazení, odsávání/filtrace prachu
- ✓ dostatečné označení a dokumentace
 - označení zařízení (název, inv. číslo, ip adresa, mac adresa, kontakt na správce)
 - očíslování zásuvek a portů v patch panelech
 - topologie sítě
- ✓ používání kvalitních komponent splňujících standardy
- ✓ nasmlouvaný servis a pojištění
- ✓ pravidelné on-site a off-site zálohování klíčových dat (konfigurací, logů, účetnictví) a dokumentů (směrnic, smluv, obchodních kontaktů)
- ✓ redundantní topologie
 - záložní linky
 - mirroring
 - záložní boxy (dle stavu připravenosti – viz. níže:)
 - studená záloha
 - vlažná záloha
 - horká záloha

3. Bezpečnost sítě a služeb

- ✓ vypnutí nepotřebných služeb (každá komponenta má dělat pouze to, na co byla určena)
- ✓ zabezpečení přístupu ke zdrojům a službám
 - AAA (lokální nebo serverová – tacacs+, radius, diameter)
 - autentizace (ověření totožnosti uživatele)
 - heslem (dostatečně dlouhým a složitým)
 - biometrie (otisk prstu, oční duhovka)
 - čipové karty
 - asymetrické kryptování, elektronický podpis
 - síť důvěry – pgp
 - TTP (Trusted Third Party) - CA, pki ⁷
 - autorizace (přístupová práva ověřeného uživatele)
 - accounting (záznam činnosti uživatele)
- ✓ stanovení priorit služeb ⁸ upřednostněním kritických systémových či real-time služeb jako směrování či voice před např. běžným prohlížením webu
- ✓ správné rozdělení sítě
 - bezpečnostní zóny ⁹(internet, extranet – DMZ, intranet)
 - virtuální síť (VLAN ¹⁰) dle skupin uživatelů s podobným oprávněním či dle jiných logických seskupení (finanční oddělení, správci sítě, ostatní zaměstnanci apod.)
- ✓ perimeter security (ochrana na rozhraní bezpečnostních zón a/nebo virtuálních sítí)
 - NAT (PAT, NAPT ¹¹) – skrytí vnitřní sítě použitím privátních adres ¹² s následným překladem na jednu nebo více veřejných adres
 - firewall ¹³
 - rate limiting (icmp, udp), ochrana před útoky typu DoS, DDoS
 - antispoofing (ochrana proti podvrhování falešných dat – např. zahazování zvenčí přichozích paketů se zdrojovou adresou pocházející z vnitřní sítě apod.)
 - omezení přístupu (ACL - např. povolení zahájit komunikaci pouze z vnitřní sítě ven)
 - content filter (filtrování provozu na základě jeho obsahu) – antivirus, antispam, antimalware, omezení přístupu na některé webové stránky apod.
- ✓ endpoint security (ochrana koncových zařízení)
 - firewall, content filter
 - IPS (při výskytu příznaků naznačujících útok zablokuje odpovídající provoz)
 - IDS ¹⁴(detekuje a ohlásí případný útok, na detekci je citlivější než IPS)
- ✓ ochrana sítě před uživatelem (DHCP snooping ¹⁵, Dynamic Arp Inspection, port security ¹⁶, 802.1x, antispoofing)
- ✓ ochrana vzdáleného přístupu – ssh, VPN ¹⁷ (ipsec, ssl)
- ✓ používání zabezpečených služeb – https, smtps, imaps, dnssec
- ✓ ochrana paměťových médií (šifrováním při používání, důkladnou likvidací dat při jejich vyřazování)
- ✓ správa sítě
 - management konfigurací
 - adekvátní SW licence
 - aktualizace SW a OS
 - logování (lokálně či šifrovaně na vzdálený server)
 - přístupů a využívání služeb
 - změn stavů sítě a služeb (výpadek služby či linky, změna konfigurace, změna v

- routovací tabulky apod.)
- statistiky provozu (NetFlow ¹⁸)
- ✓ dohledové centrum
 - sledování funkčnosti síťových prvků (ping, Nagios ¹⁹, HPOpenView)
 - vyhodnocování logů, odhalování abnormalit
 - řešení problémů
- ✓ redundanci zajišťující protokoly (spanning tree ²⁰, hsrp ²¹, vrrp ²², ...)
- ✓ bezpečné směrování
 - stabilní - použití statických cest (v případě jednoduché sítě) nebo ručního vyjmenování vlastních sítí (zákaz automatické redistribuce z IGP v případě BGP ²³)
 - od důvěryhodných zdrojů (ACL, volitelná autentizace zařízení u protokolů RIP, OSPF, ISIS, BGP)
 - jen nutné směrovací informace (policy routing, distribute lists, route maps)
 - reverse-path filtering (v případech, kdy se nepoužívá asymetrické směrování)

4. Bezpečnost lidských zdrojů

- ✓ splnění předpisů BOZP
- ✓ minimalizace přístupových oprávnění (každý jen tam, kam z pozice své funkce ve firmě potřebuje)
- ✓ zastupitelnost, informovanost, komunikace
- ✓ BCM – Business Continuity Management (viz. výše na první straně)
- ✓ legislativa
- ✓ Školení
 - pravidelné a s odpovídající náplní dle daných cílových skupin
 - interní předpisy, bezpečnostní politika
 - hrozby na síti, prevence a obrana, Netiketa
 - správné ovládání IT ve firmě (OS, IS, SW a HW)

5. Specifika prostředí školy

Škola kromě toho, že poskytuje internet svým zaměstnancům, tak se také stává poskytovatelem internetu pro své studenty (zpravidla formou wifi). Je tedy nutné zdůraznit následující:

- řádné oddělení sítí (sít' pro zaměstnance, sít' v počítačových učebnách, wifi sít') a s tím související přístupová práva (nejen 802.1x) a QoS (přidělení priorit jednotlivým typům služeb)
- dodržování IT standardů (umožnění funkčního připojení zařízení od různých výrobců, zejména v případě wifi sítě a notebooků studentů)
- AAA (authentizace a autorizace jednotlivých uživatelů samostatně a nikoliv sdílená hesla)
- logování aktivit uživatelů (přihlášení, odhlášení, použité služby, ip adresy apod.)
- adekvátní bezpečnostní politika - např. (dočasné) omezení přístupu k wifi (nebo jiný postih) v případě potenciálního ohrožení sítě (přítomnost viru nebo červa na notebooku apod.) či jiného porušení pravidel jejího používání, znemožnění instalování dalšího software studenty na PC v počítačových učebnách atd.
- zabezpečení wifi sítě (WPA2, AES, 802.1x, filtrace portu 25 – tj. používání pouze vlastního školního mailserveru, atd.)

II. Doporučená technická opatření

V případě používání technologie sdíleného média (10BASE-2 apod.) či jiné zastaralé technologie provést upgrade na přepínaný ethernet alespoň 100BASE-TX (nebo rovnou 1000BASE-T). Další opatření jsou následující:

- Centrální AAA server
- Centrální firewall
- ids, ips
- konfigurovatelný switch podporující QoS a zabezpečení (dot1q, dot1p, 802.1x capable)
- zavedení synchronizace času (případně timeserver)
- syslog server
- network monitoring station
- backup server
- vlastní mailserver (imaps, smtps capable s autentizací a antispamem)
- Endstation firewall
- Endstation antivirus
- Endstation antispam

Rovněž existují prvky, které kombinují několik výše uvedených vlastností v jednom boxu (např. Router + FW + IDS + Timeserver).

III. Základní kroky nasazení

Základní kroky nasazení bezpečnostních opatření závisejí především na výsledcích bezpečnostního auditu sítě, ze kterého je patrné, která bezpečnostní opatření jsou již zavedena a která je teprve zapotřebí zavést. Obecný postup zavádění zabezpečení krok za krokem může být např. následující:

- změnit hesla (zatím pouze na dočasná)
- aplikovat FW (centrální)
- vypnutí nepotřebných služeb
- aplikovat synchronizaci času (timeserver)
- aplikovat logování (syslog server)
- network monitoring
- aplikovat zálohování (backup server)
- zabezpečení směrování (pokud je potřeba)
- v případě nutnosti update (či upgrade) OS kde je potřeba
- aplikovat FW a antivirus (anti-malware) na ostatních (koncových) stanicích
- zavedení bezpečnějších služeb (smtps, imaps, antispam na mailserveru atd.)
- update (či upgrade) používaného aplikačního SW
- v případě používání zastaralé technologie zavést přepínaný ethernet
- port security, DAI, DHCP snooping
- změna hesel na hesla trvalejšího rázu
- reverse-path filtering (pokud se nepoužívá asymetrické směrování)
- centrální AAA server
- 802.1x
- klíče, certifikáty (případně vlastní CA) , dnssec
- ezs - evidence vstupu (čipové karty), kamerový systém

IV. Cenové odhady

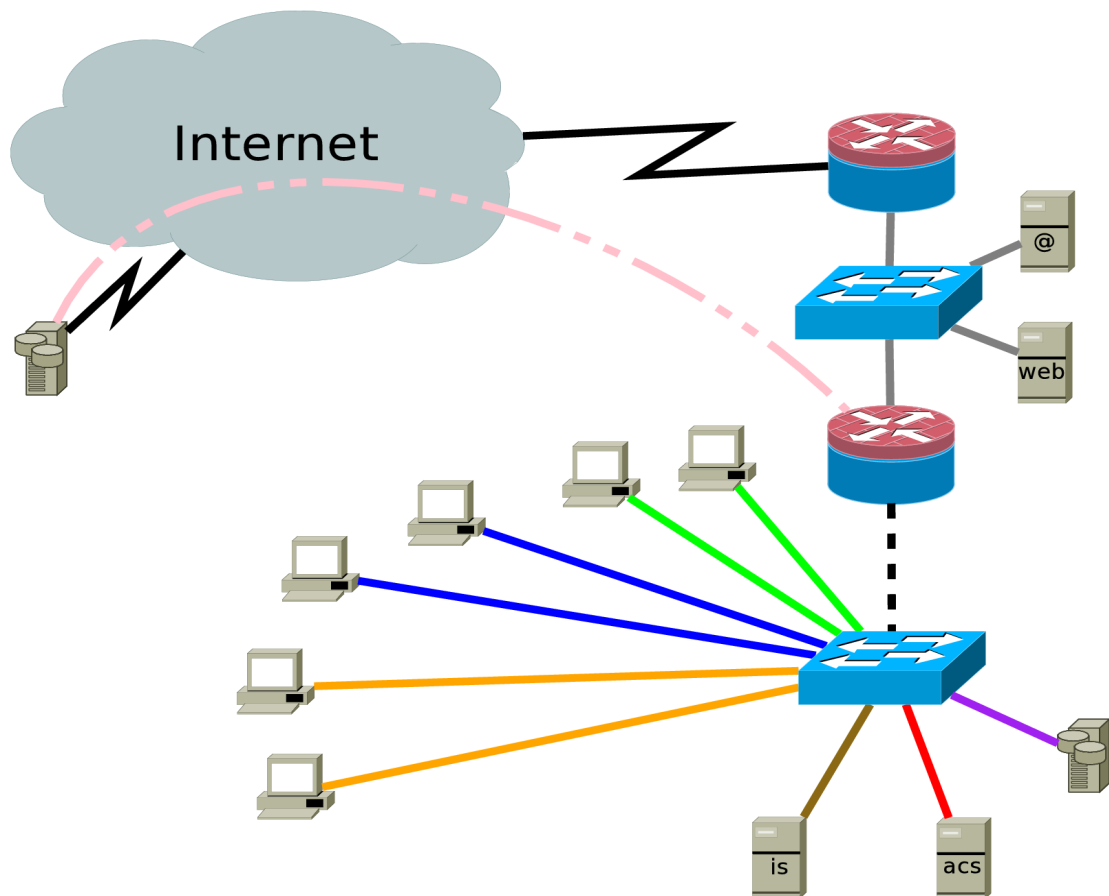
Co se cenových odhadů týká, tak zde mohou nastat výrazné cenové rozdíly v závislosti na dané implementaci (záleží na tom, zda např. zvolíme převážně PC řešení založené na Linuxu, zda budeme kombinovat několik služeb na jednom boxu či nikoliv apod.). Řešení založené na Linuxu bývá sice méně user-friendly (vyžaduje znalého administrátora), ale zato jde o řešení poměrně univerzální s velkou možností přizpůsobení (konfigurace) na míru daným podmínkám provozu (s nízkou pořizovací cenou – většinou pouze cena hw). Co se týká sdílení více služeb na jednom boxu, je to sice řešení technicky možné (a v případě omezeného množství finančních prostředků dokonce nevyhnutelné), ale z pohledu bezpečnosti nelze doporučit, neboť v bezpečnější síti by měla mít každá služba svoje vlastní železo (+ případně jedno záložní). Zpravidla se však jedná o nějaký lepší či horší kompromis. Modelový příklad by mohl být např. následující:

Předpokládáme stávající nezabezpečenou síť:

- připojení k Internetu (poslední míle včetně směrovače)
- stávající služby (email, www, dns, is)
- LAN, wifi, koncová zařízení

Nová bezpečnostní opatření (relativně jednoduchá varianta bez záložních prvků)

- upgrade na přepínaný ethernet (pokud ještě není)
 - rozvaděč ... 14000,-Kč vč. DPH (45U 600x1000)
 - UTP kabeláž ... 1800,-Kč vč. DPH (305m kat. 5e)
 - přepínač1 ... 28000,-Kč vč. DPH (48portový Linksys SGE2010)
 - přepínač2 ... 38000,-Kč vč. DPH (48portový Linksys SGE2010P with PoE)
 - cena ostatního materiálu (jako zásuvky, konektory apod.)
 - plus cena za práci ... ?
- firewall
 - varianta1 ... 53000,-Kč vč. DPH (např. ASA5510-SEC-BUN-K9)
 - varianta2 ... 20000,-Kč vč. DPH (PC s Linuxem)
- aaa server
 - varianta1 ... 200000,-Kč vč. DPH (např. HW+SW CSACS-1121-K9)
 - varianta2 ... 100000,-Kč vč. DPH (např. Radiator, Radar, RAdmin + PC s Linuxem)
 - varianta3 ... 65000,-Kč vč. DPH (např. HW+SW CSACS-5.0-EXP-K9 do 350 uživatelů)
 - varianta4 ... 20000,-Kč vč. DPH (PC s Linuxem/Freeradius)
- syslog+backup server ... 16000,-Kč vč. DPH (např. Synology DiskStation DS710+2x2GBHDD)
- případná výměna přepínače za konfigurovatelný se zabezpečením (cena viz. výše)
- případná výměna wifi ap kvůli zabezpečení (podpora WPA2, AES, 802.1x)
 - varianta1 ... 4000,-Kč vč. DPH (např. Cisco WAP4410N – jen pro malé sítě)
 - varianta2 ... 12000,-Kč vč. DPH (např. Cisco Aironet 1140)
 - doplnění varianty2 o WLC ... 160000,-Kč (např. AIR WLC4402-25-K9 pro 25 AP)
- zabezpečení koncových PC
 - varianta pro Windows ... 0,-Kč vč. DPH (např. Comodo Internet Security, Thunderbird, Ossec)
 - varianta pro Linux ... 0,-Kč vč. DPH (např. Clamav, ClamTk, Iptables, Thunderbird, Ossec)



router s firewalllem



DMZ (extranet)



Intranet VPN



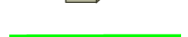
IEEE 802.1Q Trunk



Zabezp. PC (FW, ANTI*, ...)



on-site a off-site backup server



VLAN správy sítě



VLAN vedení (řed., fin. a pr.)

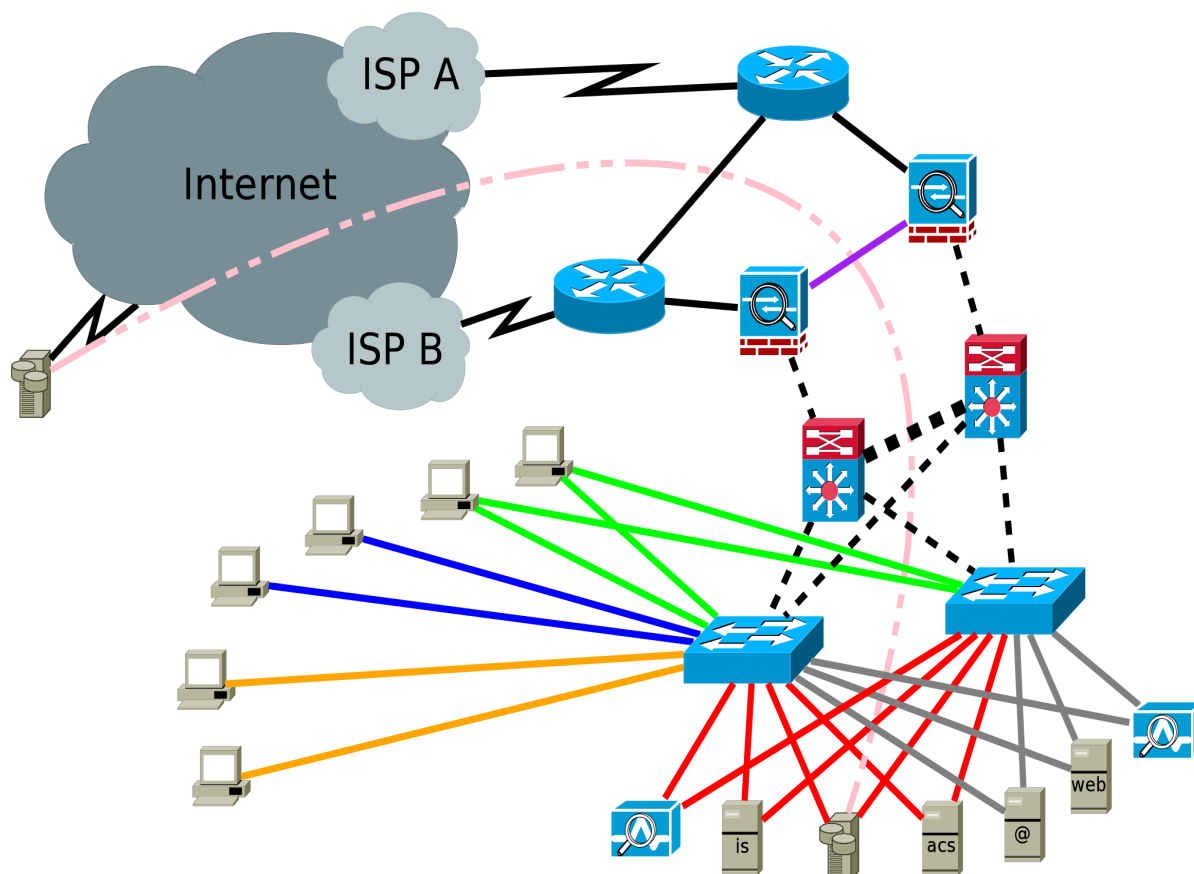




VLAN ostatních zaměstnanců



VLANy vnitřních serverů

Intranet



- DMZ
 - — — VPN pro účely zálohování
 - - - - - IEEE 802.1Q Trunk
 - ■ ■ ■ ■ LACP 802.1Q Trunk
 -  Zabezpečená PC (FW, ANTI*, ...)
 -  on-site a off-site backup server
 - VLAN správy sítě
 - VLAN vedení (řed., fin. a pr.)
 - VLAN ostatních zaměstnanců
 - VLAN vnitřních serverů
 - Firewall failover
- } Intranet

- 1 *** ISO 16085; **Risk Management: Concepts and Guidance**, Carl L. Pritchard, ESI International, USA, 2001, ISBN: 1890367303; <http://riskm-aka.blogspot.com/>
- 2 *** ISO/IEC 24762:2008; Disaster Recovery Planning: For Computers and Communication Resources, Jon William Toigo, Wiley, 1995, ISBN-10: 0471121754, ISBN-13: 978-0471121756
- 3 *** BS 25999
- 4 *** Zákon č. 133/1985 Sb.
- 5 *** ČSN EN 50131-1
- 6 *** IEC 62040-3:1999, ČSN EN 50091
- 7 *** X.509
- 8 *** IEEE 802.1P
- 9 *** RFC 2647
- 10 *** IEEE 802.1Q
- 11 *** RFC 2663
- 12 *** RFC 1918
- 13 *** RFC 2979
- 14 *** <http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>;
http://www.dmoz.org/Computers/Security/Intrusion_Detection_Systems/
- 15 ***
<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/13ew/configuration/guide/dhcp.html>
- 16 *** <http://www.enterprisenetworkingplanet.com/netsecur/print.php/3462211>
- 17 *** <http://home.zcu.cz/~ondrous/>
- 18 *** <http://www.cisco.com/go/netflow>
- 19 *** <http://www.nagios.org/>
- 20 *** IEEE 802.1D; IEEE 802.1w; IEEE 802.1s (nyní IEEE 802.1Q)
- 21 *** RFC 2281
- 22 *** RFC 3768; RFC 5798
- 23 *** RFC 1771