

Možný postup pro samostatnou praktickou kontrolu Projektu II

Před odevzdáním projektu cvičícímu doporučujeme celou síť kompletně otestovat. Následující seznam vás může navést, jak postupovat. Samozřejmě lze ověřovat i v jiném pořadí a jiným způsobem. Některé kroky tohoto seznamu pro kontrolu funkčnosti mohou (avšak nemusejí) použít i cvičící při kontrole.

Ověření správného adresování

Pro všechny segmenty zkontrolovat správnou adresu sítě, správnou masku podsítě v celé síti (s ohledem na přidělené maximální počty stanic na segmentech), zda adresy všech rozhraní na každém segmentu patří do správné IP podsítě.

Ověření fyzické konektivity

Ověřte konektivitu mezi sousedními prvky na 3. vrstvě OSI RM -ping mezi sousedy (přes Ethernet, sériovou linku, páteřní VLAN páteřní, VLAN 10)

DHCP

Testovací stanici (Microdebian) připojit do segmentu S1 (s DHCP).

Z testovací stanice zrušit případnou adresu na eth0 (ifconfig eth0 0.0.0.0), spustit DHCP klienta (dhclient eth0)

Ověřit přidělení adresy, masky a default gw klientovi (ifconfig).

Zkontrolovat debugovací výpis dhcpd (byl-li spuštěn v ladícím režimu).

Směrování

Ověřit **show ip route** na všech routerech a zkontrolovat, zda jsou ve směrovací tabulce všechny sítě, které tam mají být:

PC2, PC3:

- 5 sítí vnitřních (3 Connected, 2 z RIP), default route.

PC1:

- static default, 3 Connected, 3 vnitřní síť z RIP

C4500:

- 2 x Static route na NATovaný rozsah vaší oblasti, 3 Connected,
- OSPF interní: 2 spojovací linky páteře, 3 spojovací linky do cizích oblastí
- OSPF externí: 3 x 2 cizí NAT rozsahy

Zkontrolovat, zda jsou passive interfaces na segmentech S1 a S2.

Z testovací stanice na S1 zkusit ping na default gateway a pak do nepřímo připojených segmentů sítě. Doporučujeme postupovat postupně dál od testovací stanice, např.

- na spojovací linku PC1-PC3
- na rozhraní routeru PC2 vedoucí do segmentu S2 (VLAN10).
- na přilehlé rozhraní C4500 (tím se ověří i NAT ;-))
- na ostatní 2 rozhraní C4500
- na odlehlý konec sériové páteřní linky

- na odlehlý konec páteřní linky VLAN
- do oblasti některé spolupracující skupiny (na C4500 nebo na stroje za NAT)

NAT

Ping z testovací stanice na S1 do páteře

Ideální např. na veřejnou adresu rozhraní své C4500 přiléhajícího k oblasti, na C4500 zadat **debug ip packet** a zkontrolovat zdrojové adresy příchozích paketů, zda jsou překládány.

Přeadresovat testovací stanici na statickou adresu WWW serveru a spustit na ní triviální WWW server pro testování (/etc/init.d/thttpd restart).

Ověřit přístup na WWW server pod veřejnou statickou adresou

(např. telnet a.a.a.a 80 z C4500 (je to vnějšek NAT))

(+ zkusit zadat GET index.html HTTP /1.0 <ENTER><ENTER>, zda WWW server odpoví)

DNS

Zkontrolujte debugovací výpisy named (-g), zda nehlásí chyby v konfiguraci.

Ověření provést např. z testovací stanici na segmentu S1. Odstranit statickou adresu a vyžádat si znovu přidělení z DHCP. DHCP by jí měl přidělit i adresu DNS serveru. Zkontrolovat v souboru /etc/resolv.conf, zjistit, zda byl na stanici DNS server skutečně nastaven.

Příkazem dig (dig -t TYP jméno) zkusit získat nějaký záznam (NS nebo SOA) záznam z root domény a nějaký A záznam z poddomény. Poté vyzkoušet pro všechny záznamy vložené do DNS.

Vyzkoušet reverzní překlad IP adres (zda lze získat příslušné PTR záznamy - dig).

ACL

ACL možno ověřit buďto ve spolupráci s jinou skupinou, nebo s použitím zvláštního stroje (testovacího serveru) připojeného do přepínače přilehlého k oblasti, logicky na spojovací linku tvořenou VLAN 2, resp. VLAN 3. Na přepínači přiřaďte ještě jeden přiřadit do patřičného VLAN a tam testovací stroj připojte. Na testovacím serveru nutno spustit sshd (/etc/init.d/sshd restart), WWW server, DNS.

Při návrhu ACL pozor, pokud přiřadíte ACL na rozhraních do páteře, nesmí ACL odfiltrovat provoz směrovacího protokolu (zde OSPF) !

Otestování segmentu S2

Testovací stanici přesunout do switchu na S2 (VLAN 10), přiřaďte vhodnou IP adresu včetně ostatních parametrů sítě, zkuste ping do vnitřku oblasti (ověří směrování) a na páteřní směrovač (ověří NAT).

Spanning Tree

Na (všech) přepínačích příkazem **show spanning tree** zkontrolovat zablokované porty a cesty linek. Zkuste si nakreslit strom včetně označení portů, které jsou zablokovány a zkontrolujte, zda aktivní topologie odpovídá požadavkům.

Management adresy přepínačů

Pokuste se o přístup ma management přepínačů přes telnet (nebude hodnoceno).

