Technická specifikace připojení zákaznického zařízení k hostingové síti Master Internet s.r.o pomocí technologie ethernet

Tento popis se vztahuje na výchozí nastavení portů, pokud není technicky dohodnuto jiné nastavení, vyšší počty MAC adres nebo použití spanning tree.

Fyzická vrstva L1

Nastavení autonegociace

Připojené zařízení musí mít ethernet port nastavený pro autonegociaci přenosové rychlosti a módu duplexu. Nastavení rychlosti a módu duplexu „natvrdo“ vede v případě 100Mbps a 1000Mbps portů k duplex mismatch a k chybám v přenosu.

Linková vrstva L2

Povolené typy ethernet rámců

Směrem od zákaznického zařízení přijímáme pouze ethernet rámce s tímto ethertype

- 0x0800 - IPv4
- 0x0806 – ARP
- 0x86dd - IPv6

V případě připojení pomocí dot1q trunku

- 0x8100 – dot1q

Příslušný ethertype, který je transportován v dot1q musí být povoleného typu. Rámce s jiným ethertype můžou být zahazovány.

Maximální počet MAC adres na port

Na portech je nakonfigurována statická port security s maximálním počtem MAC adres vypočteným ze vzorce počet_přidělených_IP + 30. Ve výchozím nastavení není nastavený žádný aging naučených MAC adres.

Použití pouze ethernet unicast rámců

Z připojeného zařízení je možné posílat pouze ethernet rámce s cílovou unicast MAC adresou s výjimkou

- broadcast ARP
- ICMPv6

Zakázané L2 a link-local protokoly

- IRDP
- ICMP redirects
- **IEEE 802 Spanning Tree**
- Proprietární protkoly
    - Discovery protocols: CDP, EDP
    - VLAN/trunking protocols: VTP, DTP
- IGP (e.g. OSPF, ISIS, IGRP, EIGRP)
- FHRP – VRRP, HSRP, GLBP
- BOOTP/DHCP
- PIM-SM
- PIM-DM
- DVMRP
- ICMPv6 ND-RA
- UDLD
- L2 Keepalives

Na portech je nakonfigurován BPDU guard, posílání Spanning Tree BPDU směrem ke switchi MAI je zakázáno a vede k zavření příslušného portu. Tyto rámce jsou generovány jak hardware switchi, tak software bidges, např. zařízením br v operačním systému Linux. Před připojením je nutné tento protokol vypnout, popř. na hardwarovém switchi odfiltrovat.

Storm control

Na portech je nakonfigurován storm control. Pokud počet příchozích rámců s cílovou multicast nebo broadcast MAC překročí 100pps, port se automaticky zavře na 30s. Po této době se port opět aktivuje, pokud dojde k překročení limitu, port se opět zavře.

Síťová vrstva L3

IPv4 arp cache

Každý router v síti MAI obsahuje ARP cache, která může způsobit prodlevu při přesunu IP mezi MAC adresami v rámci jedné vlan a stejného L3 subnetu. Při změně MAC pro IP musíte routeru oznámit změnu - pomoci gratious ARP. V linuxu k tomu slouží nástroj send_arp z balíku heartbeat, po přesunu IP na nový server se na novém serveru musí spustit příkaz-

send_arp eth0 IP_KTERA_SE_PRESUNULA auto not_used not_used

Operační systémy Windows posílají gratious ARP automaticky.

Timeout ARP cache je nastaven na 4h.

IPv6 ND RA

Naše routery neposílají IPv6 ND RA. Na RS odpovídají seznamem nakonfigurovaných prefixů s flagem no-autoconfig. Toto nastavení způsobí nakonfigurování příslušných route na zařízení, ale nedojde k auto konfiguraci IPv6 adres z těchto prefixů. Vlastní IPv6 adresy je nutné na serverech nastavit staticky, stejně jako výchozí bránu.

Příklad konfigurace portu switche

Příklad konfigurace portu serveru na switchi Cisco Catalyst s IOS

```
interface GigabitEthernetYY/ZZ
 switchport access vlan XXX
 switchport mode access
 switchport nonegotiate
 switchport port-security maximum 30
 switchport port-security
 switchport port-security violation restrict
 spanning-tree portfast
 spanning-tree bpduguard enable
 storm-control action shutdown
 storm-control broadcast level pps 100
 storm-control multicast level pps 100
end
```