

* Ze zdrojových materiálů naimportovány zařízení do GNS3
* Vytvoření základního zapojení dle zadání – technologie CISCO
* Rozdělení infrastruktury do VLAN
  + 10 – DMZ
  + 20 – Intranet
  + 30 –VLAN-HOST
  + 40 –Interní síť (zaměstnanci IP-01,ZAM-PC1..)
  + 50 –WiFi-Host (jako AP vložen FIREFOX stroj – bude nahrazen)
  + 60 –WiFi-Zamestnanec (jako AP vložen FIREFOX stroj – bude nahrazen)
  + 100 –Management
* Nastavení IP adres (pevných i DHCP), DHCP (výpůjčky..), nastavení routování a připojení do internetu
* Nastavení pravidel provozu – Access listy
* Nastavení 802.1X, AAA serveru, RADIUS serveru a přidání nového uživatele it-novak
* Do VLAN Intranet přidán stroj ZABBIXserver a instalace ZABBIX software pro monitoring sítě
* Na aktivních zařízeních nastaveno zabezpečení přístupu k administraci (SSH, nastavení hesel)

Veškerý postup a nastavení jednotlivých prvků infrastruktury je uvedeno následně ve formě výpisu *running-config* (router + switche) a editace nastavení jednotlivých strojů.

Připojení dalšího AP k jakémukoliv portu na switchi STAFF:

Na Radius serveru bychom nastavily ověření uživatele (AP) a po ověření dle nastaveného mapování uživatelů tento AP zařadily do příslušné VLANy bez závislosti na použitého portu.   
Je nutno nastavit staticky IP na AP rezervovanou pro danou VLANU (VLAN 50 nebo 60).

**Nastavení zařízení:**

Router Cisco: **CoreRouter**

hostname CoreRouter

boot-start-marker

boot-end-marker

enable secret 5 $1$2Nkw$qnKnZnEHFFRZ3ttdAU8uK/

aaa new-model

aaa session-id common

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

no ip icmp rate-limit unreachable

ip dhcp excluded-address 192.168.50.0 192.168.50.10

ip dhcp excluded-address 192.168.60.0 192.168.60.10

ip dhcp excluded-address 10.0.10.0 10.0.11.0

ip dhcp excluded-address 192.168.100.0 192.168.100.19

ip dhcp excluded-address 192.168.100.21 192.168.100.30

ip dhcp excluded-address 192.168.255.0 192.168.255.9

ip dhcp excluded-address 192.168.255.11 192.168.255.19

ip dhcp excluded-address 192.168.255.21 192.168.255.60

ip dhcp excluded-address 192.168.12.0 192.168.12.50

ip dhcp pool DMZ

network 192.168.100.0 255.255.255.128

ip dhcp pool Intranet

network 192.168.255.0 255.255.255.128

default-router 192.168.255.1

dns-server 192.168.122.1

ip dhcp pool VLAN-HOST

network 10.0.10.0 255.255.254.0

dns-server 192.168.122.1

default-router 10.0.10.1

ip dhcp pool Interni

network 192.168.12.0 255.255.252.0

dns-server 192.168.122.1

default-router 192.168.12.1

ip dhcp pool WiFi-Host

network 192.168.50.0 255.255.255.0

dns-server 192.168.122.1

default-router 192.168.50.1

ip dhcp pool WiFi-Zamestnanec

network 192.168.60.0 255.255.252.0

dns-server 192.168.122.1

default-router 192.168.60.1

ip dhcp pool IntranetWWW

host 192.168.255.10 255.255.255.128

client-identifier 015a.eeff.7333.22

ip dhcp pool NAS1

host 192.168.255.20 255.255.255.128

client-identifier 011e.b10e.5fb5.98

ip dhcp pool WEBserver

host 192.168.100.20 255.255.255.248

client-identifier 01fa.235d.a3a5.12

ip dhcp pool IT-01

host 192.168.12.51 255.255.252.0

client-identifier 010c.929f.31c9.22

dns-server 192.168.122.1

default-router 192.168.12.1

ip dhcp pool AutomatCola

host 10.0.11.1 255.255.254.0

client-identifier 0100.5079.6668.00

dns-server 192.168.122.1

default-router 10.0.10.1

no ip domain lookup

ip domain name utb.local

ip cef

no ipv6 cef

vlan ifdescr detail

multilink bundle-name authenticated

username IT-01 secret 5 $1$DKwH$RtVBXg1iNJ/eNyq3FdMuK/

redundancy

no cdp log mismatch duplex

ip tcp synwait-time 5

interface GigabitEthernet0/0

ip address dhcp

ip nat outside

ip virtual-reassembly in

duplex auto

speed auto

media-type rj45

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

media-type rj45

interface GigabitEthernet0/1.10

encapsulation dot1Q 10 native

ip address 192.168.100.1 255.255.255.240

ip access-group DMZports out

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/2

no ip address

duplex auto

speed auto

media-type rj45

interface GigabitEthernet0/2.10

encapsulation dot1Q 10 native

ip address 192.168.100.17 255.255.255.248

ip access-group DMZports out

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/3

no ip address

duplex auto

speed auto

media-type rj45

interface GigabitEthernet0/3.10

encapsulation dot1Q 10 native

ip address 192.168.100.25 255.255.255.248

ip access-group DMZports out

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/4

no ip address

duplex auto

speed auto

media-type rj45

interface GigabitEthernet0/4.30

encapsulation dot1Q 30

ip address 10.0.10.1 255.255.254.0

ip access-group VLAN-HOST2Internet in

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/4.100

encapsulation dot1Q 100

ip address 192.168.200.98 255.255.255.128

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/5

no ip address

duplex auto

speed auto

media-type rj45

interface GigabitEthernet0/5.20

encapsulation dot1Q 20

ip address 192.168.255.1 255.255.255.128

ip access-group Zabbix out

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/5.40

encapsulation dot1Q 40

ip address 192.168.12.1 255.255.252.0

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/5.50

encapsulation dot1Q 50

ip address 192.168.50.1 255.255.255.0

ip access-group WiFiHost2Internet in

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/5.60

encapsulation dot1Q 60

ip address 192.168.60.1 255.255.252.0

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/5.100

encapsulation dot1Q 100

ip address 192.168.200.129 255.255.255.128

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/6

no ip address

shutdown

duplex auto

speed auto

media-type rj45

interface GigabitEthernet0/7

no ip address

shutdown

duplex auto

speed auto

media-type rj45

interface GigabitEthernet0/8

no ip address

shutdown

duplex auto

speed auto

media-type rj45

interface GigabitEthernet0/9

no ip address

shutdown

duplex auto

speed auto

media-type rj45

ip forward-protocol nd

no ip http server

no ip http secure-server

ip nat inside source list 1 interface GigabitEthernet0/0 overload

ip route 0.0.0.0 0.0.0.0 192.168.122.1

ip ssh version 2

ip access-list extended DMZports

deny ip 10.0.10.0 0.0.0.127 any

deny ip 192.168.50.0 0.0.0.255 any

permit udp any any eq domain

permit tcp any any eq 443

permit tcp any any eq 993

permit tcp any any eq 587

permit tcp any any eq smtp

permit tcp host 192.168.12.51 any eq 22

permit tcp host 192.168.12.51 any eq 9090

deny ip any any

ip access-list extended VLAN-HOST2Internet

deny ip 10.0.10.0 0.0.1.255 192.168.255.0 0.0.0.127

deny ip 10.0.10.0 0.0.1.255 192.168.100.0 0.0.0.127

deny ip 10.0.10.0 0.0.1.255 192.168.200.0 0.0.0.255

deny ip 10.0.10.0 0.0.1.255 192.168.12.0 0.0.3.255

deny ip 10.0.10.0 0.0.1.255 192.168.50.0 0.0.0.255

permit ip any any

ip access-list extended WiFiHost2Internet

deny ip 192.168.50.0 0.0.0.255 10.0.10.0 0.0.0.127

deny ip 192.168.50.0 0.0.0.255 192.168.255.0 0.0.0.127

deny ip 192.168.50.0 0.0.0.255 192.168.100.0 0.0.0.127

deny ip 192.168.50.0 0.0.0.255 192.168.60.0 0.0.3.255

deny ip 192.168.50.0 0.0.0.255 192.168.200.0 0.0.0.255

deny ip 192.168.50.0 0.0.0.255 192.168.12.0 0.0.3.255

permit ip any any

ip access-list extended Zabbix

permit tcp host 192.168.12.51 host 192.168.255.29 eq 22

permit tcp host 192.168.12.51 host 192.168.255.29 eq 443

permit udp any host 192.168.255.29 eq snmp

permit udp any host 192.168.255.29 eq snmptrap

deny ip any host 192.168.255.29

permit ip 192.168.60.0 0.0.3.255 192.168.255.0 0.0.0.127

permit ip 192.168.255.0 0.0.0.127 192.168.60.0 0.0.3.255

permit ip 192.168.12.0 0.0.3.255 192.168.255.0 0.0.0.127

permit ip 192.168.255.0 0.0.0.127 192.168.12.0 0.0.3.255

deny ip any any

ipv6 ioam timestamp

access-list 1 permit 10.0.10.0 0.0.1.255

access-list 1 permit 192.168.255.0 0.0.0.127

access-list 1 permit 192.168.50.0 0.0.0.255

access-list 1 permit 192.168.60.0 0.0.3.255

access-list 1 permit 192.168.200.0 0.0.0.255

access-list 1 permit 192.168.12.0 0.0.3.255

access-list 10 permit 192.168.12.51

control-plane

line con 0

exec-timeout 0 0

privilege level 15

password heslo

logging synchronous

line aux 0

exec-timeout 0 0

privilege level 15

password heslo

logging synchronous

line vty 0 4

access-class 10 in

transport input ssh

Switch: **PublicSW**

hostname PublicSW

enable secret 5 $1$ckjt$ljRJ/4qrlUFn1ueGVK6yT.

username IT-01 secret 5 $1$rP0w$ygaYupFpqMChWXHuBZEa20

aaa new-model

aaa session-id common

ip domain-name utb.local

ip cef

no ipv6 cef

errdisable recovery cause psecure-violation

errdisable recovery interval 120

spanning-tree mode pvst

spanning-tree extend system-id

vlan internal allocation policy ascending

interface GigabitEthernet0/0

description TrunkToRouter

switchport trunk encapsulation dot1q

switchport mode trunk

media-type rj45

negotiation auto

spanning-tree portfast edge trunk

ip dhcp snooping trust

interface GigabitEthernet0/1

switchport access vlan 30

switchport mode access

switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security mac-address sticky 0050.7966.6800

switchport port-security

media-type rj45

negotiation auto

interface GigabitEthernet0/2

switchport access vlan 30

switchport mode access

switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security mac-address sticky 0c92.9f35.3900

switchport port-security

ip access-group 101 in

media-type rj45

negotiation auto

interface GigabitEthernet0/3

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet1/0

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet1/1

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet1/2

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet1/3

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet2/0

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet2/1

shutdown

media-type rj45

negotiation auto

interface Vlan30

ip address 10.0.10.2 255.255.254.0

interface Vlan100

ip address 192.168.200.99 255.255.255.224

ip forward-protocol nd

no ip http server

no ip http secure-server

ip route 0.0.0.0 0.0.0.0 192.168.200.98

ip ssh version 2

access-list 10 permit 192.168.12.51

access-list 101 deny ip 10.0.10.0 0.0.1.255 host 10.0.11.1

access-list 101 permit ip any any

line con 0

password heslo

line aux 0

password heslo

line vty 0 4

access-class 10 in

transport input ssh

Switch: **STAFF**

hostname STAFF

enable secret 5 $1$mUpj$SYkrPQu93WZYMYSN4TRvx0

username IT-01 secret 5 $1$j4e7$SIA.RwQJHPvTFKyQ0dmV10

aaa new-model

aaa group server radius gns3group

server name radius1

aaa authentication dot1x default group gns3group local

aaa session-id common

ip domain-name utb.local

ip cef

no ipv6 cef

dot1x system-auth-control

errdisable recovery cause psecure-violation

errdisable recovery interval 120

spanning-tree mode pvst

spanning-tree extend system-id

vlan internal allocation policy ascending

interface GigabitEthernet0/0

description TrunkToRouter

switchport trunk encapsulation dot1q

switchport mode trunk

media-type rj45

negotiation auto

ip dhcp snooping trust

interface GigabitEthernet0/1

switchport access vlan 40

switchport mode access

switchport port-security mac-address 0c92.9f31.c922

switchport port-security

media-type rj45

negotiation auto

interface GigabitEthernet0/2

switchport access vlan 40

switchport mode access

switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security mac-address sticky 0c92.9f89.6301

switchport port-security

media-type rj45

negotiation auto

authentication port-control auto

dot1x pae authenticator

interface GigabitEthernet0/3

description TrunkSwichSwich

switchport trunk encapsulation dot1q

switchport mode trunk

media-type rj45

negotiation auto

interface GigabitEthernet1/0

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet1/1

switchport access vlan 50

switchport mode access

switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security mac-address sticky 0c92.9f78.ad00

switchport port-security

media-type rj45

negotiation auto

interface GigabitEthernet1/2

switchport access vlan 60

switchport mode access

switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security mac-address sticky 0c92.9f4d.cf00

switchport port-security

media-type rj45

negotiation auto

interface GigabitEthernet1/3

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet2/0

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet2/1

shutdown

media-type rj45

negotiation auto

interface Vlan100

ip address 192.168.200.199 255.255.255.128

ip default-gateway 192.168.200.129

ip forward-protocol nd

no ip http server

no ip http secure-server

ip route 0.0.0.0 0.0.0.0 192.168.200.129

ip ssh version 2

access-list 10 permit 192.168.12.51

radius server radius1

address ipv4 192.168.255.30 auth-port 1812 acct-port 1813

key gns3

line con 0

password heslo

line aux 0

password heslo

line vty 0 4

access-class 10 in

transport input ssh

Switch: **INTRA**

hostname INTRA

enable secret 5 $1$X8Yf$2RpQG.4ecc07lx8Ny/RBl/

username IT-01 secret 5 $1$tmBa$gvxHOp8pE1388zvXhPDNE.

aaa new-model

aaa session-id common

ip arp inspection vlan 20

ip arp inspection validate src-mac

ip domain-name utb.local

ip cef

no ipv6 cef

errdisable recovery cause psecure-violation

errdisable recovery cause arp-inspection

spanning-tree mode pvst

spanning-tree extend system-id

vlan internal allocation policy ascending

interface GigabitEthernet0/0

description TrunkSwichSwich

switchport trunk encapsulation dot1q

switchport mode trunk

ip arp inspection trust

media-type rj45

negotiation auto

ip dhcp snooping trust

interface GigabitEthernet0/1

switchport access vlan 20

switchport mode access

switchport port-security mac-address 5aee.ff73.3322

switchport port-security

media-type rj45

negotiation auto

interface GigabitEthernet0/2

switchport access vlan 20

switchport mode access

switchport port-security mac-address 1eb1.0e5f.b598

switchport port-security

media-type rj45

negotiation auto

interface GigabitEthernet0/3

switchport access vlan 20

switchport mode access

switchport port-security mac-address d664.d99e.59b8

switchport port-security

media-type rj45

negotiation auto

interface GigabitEthernet1/0

switchport access vlan 20

switchport mode access

switchport port-security mac-address d631.837b.7687

switchport port-securitymedia-type rj45

negotiation auto

interface GigabitEthernet1/1

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet1/2

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet1/3

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet2/0

shutdown

media-type rj45

negotiation auto

interface GigabitEthernet2/1

shutdown

media-type rj45

negotiation auto

interface Vlan100

ip address 192.168.200.200 255.255.255.128

ip default-gateway 192.168.200.129

ip forward-protocol nd

no ip http server

no ip http secure-server

ip route 0.0.0.0 0.0.0.0 192.168.200.129

ip ssh version 2

access-list 10 permit 192.168.12.51

line con 0

password heslo

line aux 0

password heslo

line vty 0 4

access-class 10 in

transport input ssh

**Servery:**

DNSpublic:

auto eth0

iface eth0 inet static

address 192.168.255.29

netmask 255.255.255.128

gateway 192.168.255.1

up echo nameserver 192.168.122.1 > /etc/resolv.conf

WEBserver:

auto eth0

iface eth0 inet dhcp

hwaddress ethe fa:23:5d:a3:a5:12

pre-up ifconfig eth0 hw ether fa:23:5d:a3:a5:12

MAILserver:

auto eth0

iface eth0 inet static

address 192.168.100.30

netmask 255.255.255.248

gateway 192.168.255.1

up echo nameserver 192.168.122.1 > /etc/resolv.conf

IntranetWWW:

auto eth0

iface eth0 inet dhcp

hwaddress ethe 5a:ee:ff:73:33:22

pre-up ifconfig eth0 hw ether 5a:ee:ff:73:33:22

NAS1:

auto eth0

iface eth0 inet dhcp

hwaddress ethe 1e:b1:0e:5f:b5:98

pre-up ifconfig eth0 hw ether 1e:b1:0e:5f:b5:98

AAA:

auto eth0

iface eth0 inet static

address 192.168.255.30

netmask 255.255.255.128

gateway 192.168.255.1

up echo nameserver 192.168.122.1 > /etc/resolv.conf

hwaddress ethe d6:64:d9:9e:59:b8

pre-up ifconfig eth0 hw ether d6:64:d9:9e:59:b8

ZABBIXserver:

auto eth0

iface eth0 inet static

address 192.168.255.29

netmask 255.255.255.128

gateway 192.168.255.1

up echo nameserver 192.168.122.1 > /etc/resolv.conf

hwaddress ethe d6:31:83:7b:76:87

pre-up ifconfig eth0 hw ether d6:31:83:7b:76:87

**Počítače:**

Automat-Cola:

dhcp

HW: 00:50:79:66:68:00

IT-01:

HW: 0c:92:9f:31:c9:22

**ZABBIX:**

ZABBIXserver

**Účet na radius serveru:**

Přidání nového účtu na RADIUS server:

nano /etc/freeradius/3.0/users

přidat za první dva uživatele (alice a bob)

it-novak Cleartext-Password := "65+123sPL-22"

Reply-Message = "Hello, %{User-Name}"