Chapter 6: Enterprise Internet Connectivity

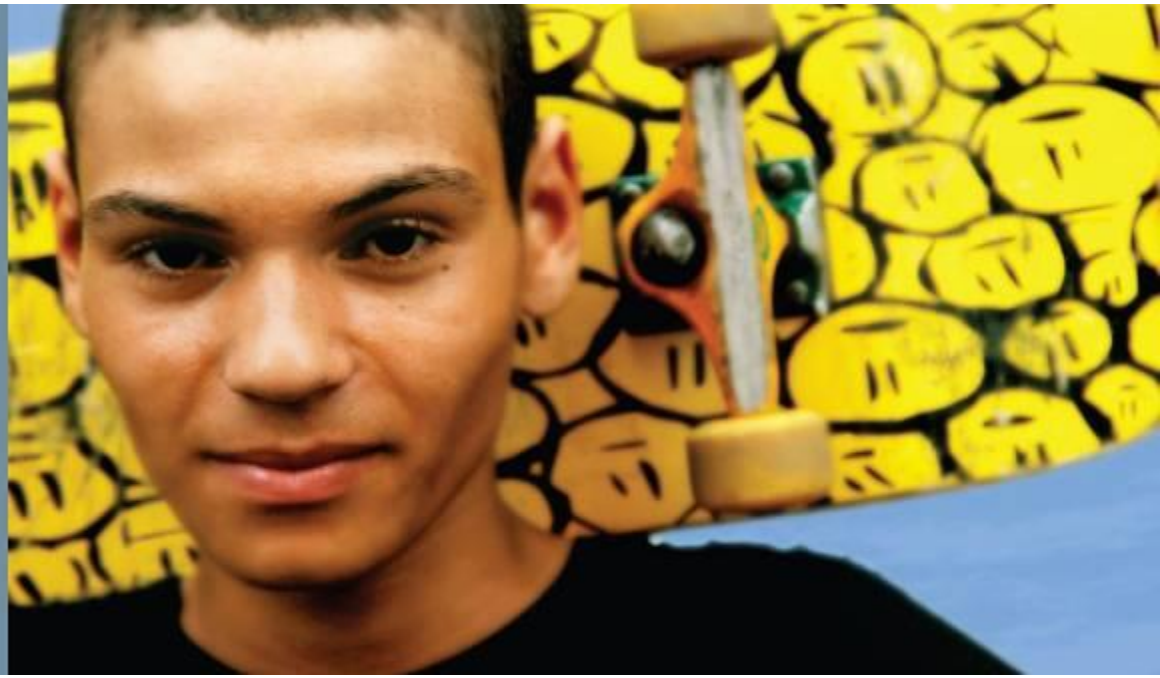
CCNP ROUTE: Implementing IP Routing

Cisco | Networking Academy®
Mind Wide Open™

Čo nás čaká

- Plánovanie podnikovej internetovej konektivity
- Single-Homed IPv4 Internet Connectivity
- Single-Homed IPv6 IPv6 Internet Connectivity
- Odolnosť internetovej konektivity
  - Resilience

Plánovanie podnikovej internetovej konektivity



Plánovanie podnikovej internetovej konektivity

- Pripojenie podnikov k ISP na ISP
  - Splnenie požiadaviek ako
    - Verejný IP adresný priestor
      - RIR -> ISP -> customer
- Odlišné typy riešení konektivity na ISP
  - Prepojenie linkou medzi Enterprise-to-ISP daným typom a BW
  - Redundancia pripojenia
  - Smerovací protokol
- Prideľovanie verejných IP adries
  - Závislé od ISP
  - Nezávislé od ISP
- Použitie autonomous system numbers (ASN)

Pripojenie podnikovej siete na ISP

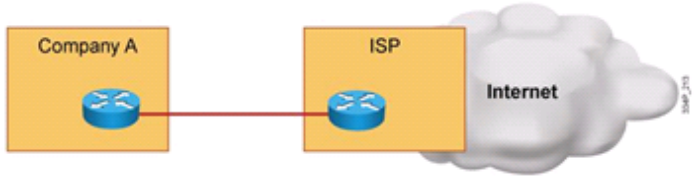
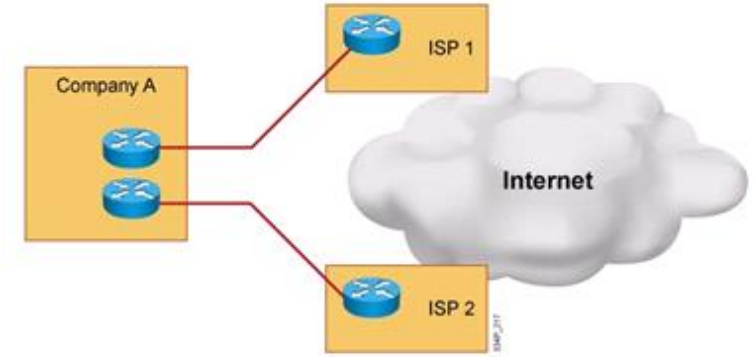
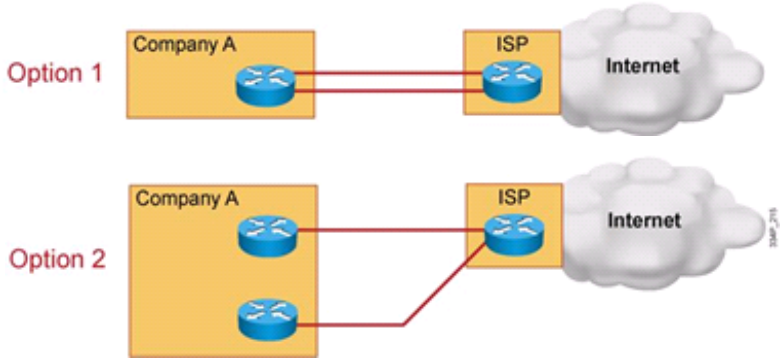
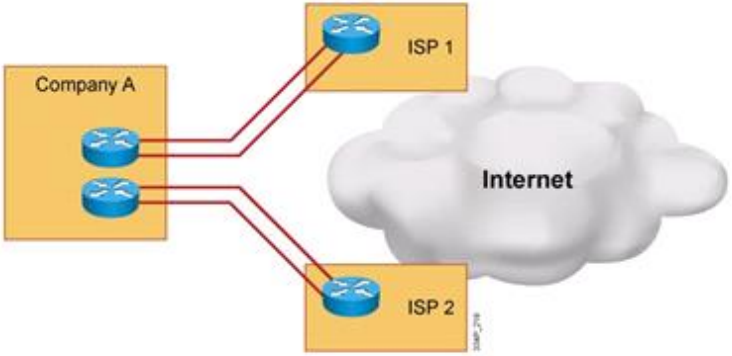
Požiadavky podnikov na konektivitu

- **V smere Outbound**
  - Vo výnimočných prípadoch stačí jednocestná (jednobodová) konektivita
    - Otázka redundancie
  - Použitie privátneho IPv4 adresného priestoru vo vnútri
  - Potreba nasadiť NAT
    - Konektivita smerom od vnútorných klientov v private priestore na servery-služby v public priestore
- **V smere Inbound**
  - Potreba prístupu externých klientov na podnikové služby dnu
    - Vhodné riešiť konektivity cez dve linky
  - Potreba verejného aj privátneho adresného priestoru
    - Otázky okolo NAT, routingu, bezpečnosti

Riešenia konektivity podnikových sietí na ISP

- **Pri pripojení zákazníka na ISP potreba zamyslieť sa**
  - **Redundancia linky**
    - Redundancia linky na router ISP zvyšuje odolnosť konektivity
  - **Redundancia okrajového (Edge) zariadenia**
    - Nasadenia redundantných okrajových zariadení (router, firewall) zvyšuje odolnosť voči výpadkom
  - **Redundancia ISP**
    - Ak prevádzkujeme kritické servery/služby/aplikácie alebo prístup k ním je nevyhnutný
    - Potreba chrániť sa voči výpadkom na strane ISP
    - => je potrebná redundancia a mať dvoch ISP

Možnosti pripojenia na ISP (medzi AS)

Connecting to One ISP	Connecting to Two or more ISPs
Single-homed 	**Multihomed** 
Dual-homed 	**Dual-multihomed** 

Redundancia ISP

- **Single-homed**
  - With a connection to a single ISP when no link redundancy is used, the customer is *single-homed.* Single-homed ISP connectivity is used in cases when a loss in Internet connectivity is not problematic to a customer.
- **Dual-homed**
  - With a connection to a single ISP, redundancy can be achieved if two links toward the same ISP are used effectively.
  - There are two options for dual homing: Both links can be connected to one customer router, or to enhance the resiliency further, the two links can terminate at separate routers in the customer's network.
  - In either case, routing must be properly configured to allow both links to be used.

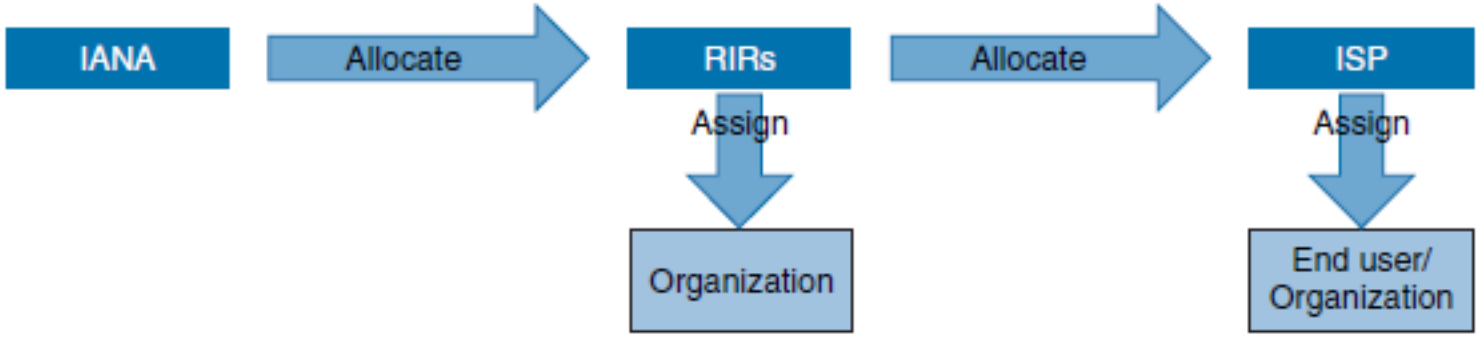
Redundancia ISP

- **Multihomed**
  - With connections to multiple ISPs, redundancy is built in to the design.
  - Connections from different ISPs can terminate on the same router, or on different routers to further enhance the resiliency.
  - The customer is responsible for announcing its own IP address space to upstream ISPs, but should avoid forwarding any routing information between ISPs (otherwise the customer becomes a transit provider between the two ISPs). The routing used must be capable of reacting to dynamic changes. Multihoming also allows load balancing of traffic between ISPs.
- **Dual multihomed**
  - To enhance the resiliency further with connections to multiple ISPs, a customer can have two links toward each ISP.

Prideľovanie Public IP Adresného priestoru

Internet Assigned Numbers Authority (IANA):

- Manažuje globálne rozsahy adresného priestoru a prideľovanie IPv4 aj IPv6 adries
  - Poskytuje ho RIR-om
- Manažuje priestor AS (Autonomous system numbers)
  - Poskytuje ho RIR-om
- Riadi Domain Name Service (DNS) root zónu
- Riadi IP číslovací systém
  - v spolupráci so štandardardizačnými organizáciami



Regional Internet Registries - RIRs

- **African Network Information Centre (AfriNIC)**
  - Zodpovedný za Afriku
- **Asia Pacific Network Information Centre (APNIC)**
  - Asia Pacific región
- **American Registry for Internet Numbers (ARIN)**
  - Kanada, United States, niekoľko ostrovov v Karibskom mori a Severnom atlantickom oceáne
- **Latin American and Caribbean IP Address Regional Registry (LACNIC)**
  - Latin America a časť Karibiku
- **Reséaux IP Européens Network Coordination Centre (RIPE NCC)**
  - Europe, Middle East, Central Asia

Pridelenie Public IP adresného priestoru

- **Provider Aggregatable (PA) Address Space**
  - A PA block of IP addresses is used in simple topologies, where no redundancy is needed.
  - PA address space is assigned by the ISP to its customer, from its address space.
  - If the customer changes its ISP, the new ISP will give the customer a new PA address space, and all devices with public IP addresses will have to be renumbered; the old address space cannot be transferred to the new.

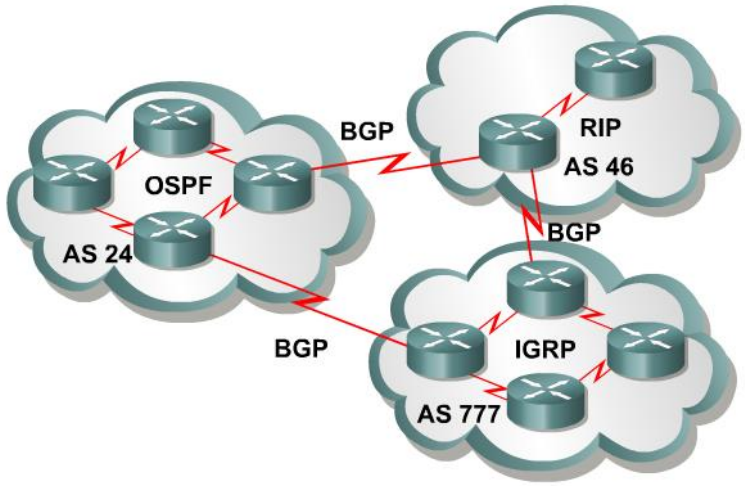
Pridelenie Public IP adresného priestoru

- **Provider-Independent Address Space**
  - For a multihomed connection, a PI address space is required because the enterprise network needs to be independent of the ISP's address space.
  - The PI address space must be acquired from an RIR; it is assigned directly to an organization by the RIR, and is not related to any ISP.
  - This address space can be routed through other service providers, resulting in more flexibility when planning connections to ISPs and when migrating between service providers.
  - After successfully processing an address space request, the RIR assigns the PI address space and a public autonomous system number (ASN) (described in the next section) that uniquely defines the enterprise's network and its address spaces.
  - This ASN is not related to any ISP.
  - The enterprise then configures their Internet gateway routers to advertise the newly assigned IP address space to neighboring ISPs; the Border Gateway Protocol (BGP) is typically used for this task.

Pridelenie Public ASN – čo je ASN

- Autonómny systém (AS) je skupina sietí a smerovačov, ktorá používajú spoločnú smerovaciu politiku a patria pod spoločnú administratívnu doménu
  - Smerovacia politika: spôsob výberu ciest do rôznych cieľov, filtrovanie smerovacích informácií, oznamovanie smerov...
  - Administratívna doména: dosah administratívnej právomoci správcu
- Vo vnútri AS môže pracovať jeden alebo niekoľko IGP
  - AS však ako celok patrí spravidla jednej organizácii
- Zvonku je AS vnímaný ako jedna nerozdelená entita
  - Všetky členské siete v AS sú v ňom z pohľadu iných AS priamo dostupné
- V prípade, že je AS pripojený na verejný Internet s použitím EGP (BGP)
  - AS musí byť pridelené IANA

Pridelenie Public ASN



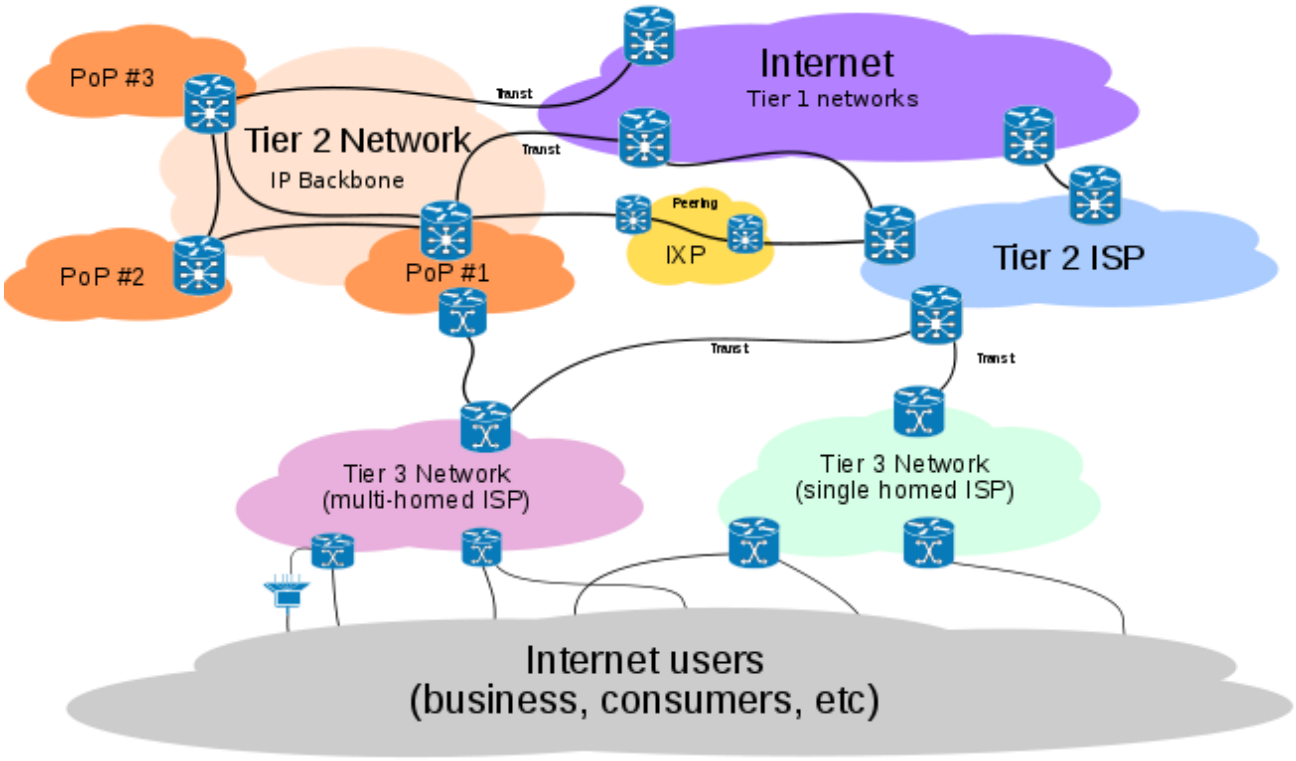
Internet je skupina navzájom poprepájaných Autonómnych systémov (AS)

- AS sú číslované – ASN
  - Čísla AS rozdeľuje IANA na regionálne internetové registre,
    - Tí následne prideľujú AS jednotlivým žiadateľom
  - V súčasnosti sa používajú 2B čísla (0 – 65535)
  - RFC 4893 špecifikuje použitie 4B čísel (v dekadickom zápise 2B.2B)
  - Časť priestoru od 64512 po 65535 je vyhradená pre privátne ASN
- IANA nástojí na tom, aby organizácie, ktoré chcú mať vlastné číslo AS, avšak majú iba jediného ISP a zdieľajú jeho smerovacie politiky, zásadne používali privátne ASN
  - Privátne čísla AS sa objavujú len v sieti ISP a sú zamenené za ASN providera, keď sa prenášajú do iných AS

Rezervované ASN

- IANA definuje dva ASN rozsahy pre **privátne účely**
  - 64,512 po 65,534
  - 4,200,000,000 po 4,294,967,294 (64,086.59904 po 65,535.65534)
- A dva rozsahy pre ukážky, dokumentácie a príklady:
  - 64,496 po 64,511
  - 65,536 po 65,551

Štruktúra Internetu - AS infraštruktúra



- Jednotlivé AS (ISP AS) sa prepájajú cez Internet Packet Exchange (IPX) Gateways v tzv. Internet Exchange Points (IXP)
  - IXP je priamy prepoj, cez ktorý si ISP vymieňajú navzájom svoje dáta
    - A redukujú množstvo, ktoré musia posielať cez svojich *tranzitných* providerov
    - Peering:
      - dobrovoľný prepoj AS za účelom vzájomnej výmeny dát („*ak prepošleš moje ja prepošlem tvoje*“)

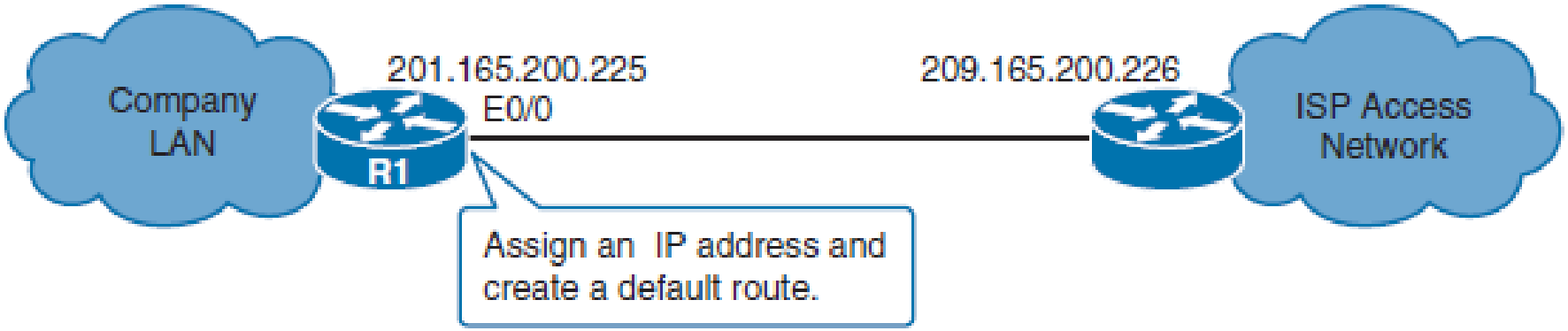
Budovanie Single-Homed IPv4 Internet konektivity

Popíšeme si

- Pri zakladaní Single-Homed IPv4 Internet konektivity
  - Ako sa konfiguruje smerovač s ISP pridelenou
    - staticky konfigurovanou IP adresou
    - DHCP pridelenou IP adresou
  - Vysvetlenie DHCP činnosti a ako použiť smerovač ako DHCP server a relay agent
  - Vysvetlenie typov NAT
  - Popíšeme NAT virtual interface (NVI) , jeho konfiguráciu a overenie

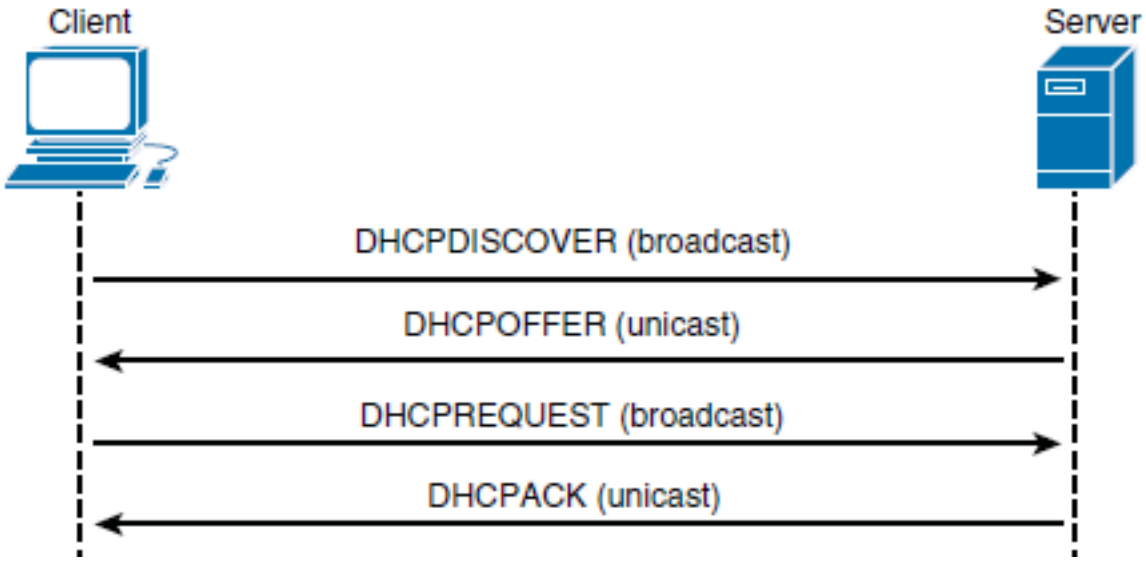
Konfigurácia statickej IPv4 adresy

- **Konfigurácia smerovača pre staticky pridelenú IPv4**
  - **Step 1**. Staticky prideľ IP na rozhranie k ISP
  - **Step 2.** Konfiguruj default route
    - Ktorá rieši doručenie Internetovej premávky na smerovač ISP.




```
R1(config)# interface Ethernet 0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.224
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.226
```

DHCP Operation

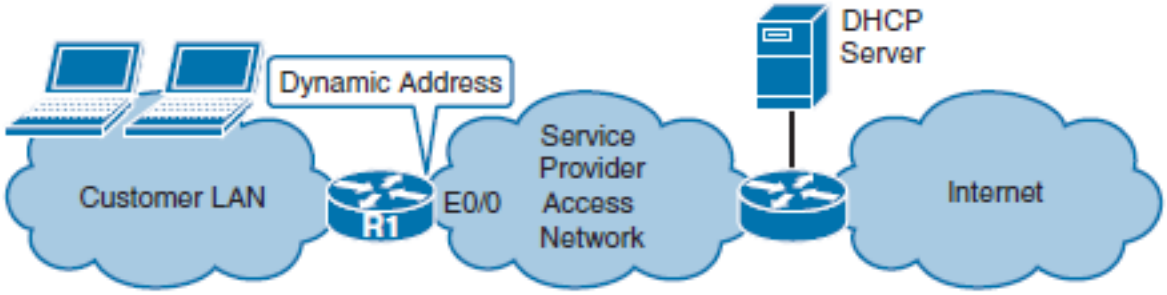


Four other DHCP messages are possible:

- **DHCPDECLINE:** A message sent from a client to a server indicating that the address is already in use
- **DHCPNAK:** A message sent from a server indicating that it is refusing a client's request for configuration
- **DHCPRELEASE:** A message sent from a client indicating to a server that it is giving up a lease
- **DHCPINFORM:** A message sent from a client indicating that it already has an IPv4 address, but is requesting other configuration parameters from the DHCP server, such as a DNS address

Získanie IPv4 adresy od poskytovateľa cez DHCP

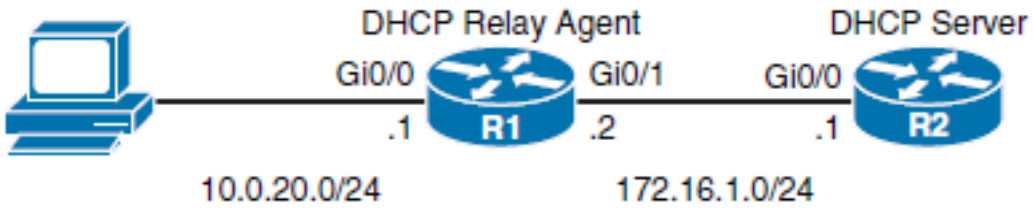
- Pri dynamickej konfigurácii
  - Treba povoliť DHCP klienta na smerovači k ISP
  - Cez DHCP sa získa IP, maska, default route, DNS a ďalšie




```
R1(config)# interface Ethernet 0/0
R1(config-if)# ip address dhcp
R1(config-if)# end

R1# show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "static", distance 254, metric 0, candidate default path
  Routing Descriptor Blocks:
  * 209.165.200.226
      Route metric is 0. traffic share count is 1
```

Konfigurácia smerovača ako DHCP Server a DHCP Relay Agent




```
R2(config)# ip dhcp pool MYLAN
R2(dhcp-config)# network 10.0.20.0 255.255.255.0
R2(dhcp-config)# default-router 10.0.20.1
R2(dhcp-config)# lease 2
R2(dhcp-config)# exit
R2(config)# ip dhcp excluded-address 10.0.20.1 10.0.20.49
```

```
R1(config)# interface gi0/0
R1(config-if)# ip helper-address 172.16.1.1
```

NAT

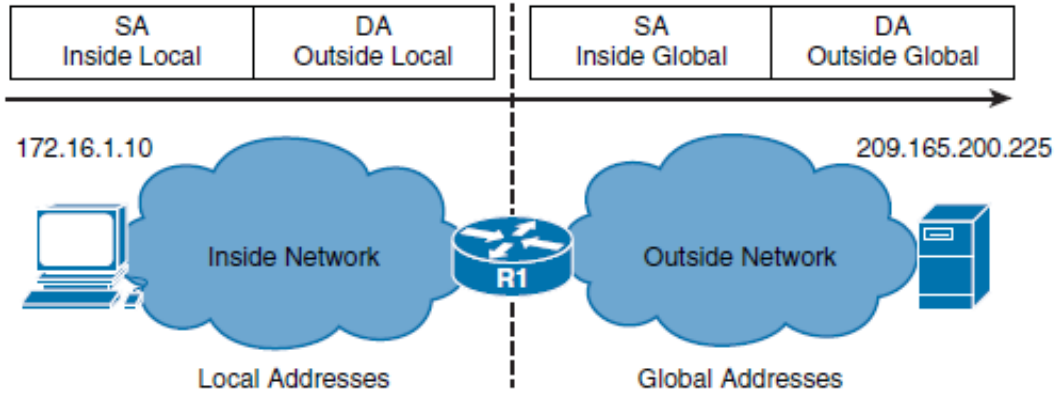
- NAT is usually implemented on border devices such as firewalls or routers, which allows devices within an organization to have private addresses.
- NAT translates private addresses to public addresses and vice versa, keeping a mapping between the two for return traffic.
- NAT can be configured to translate all private addresses to only one public address or to pick from a pool of public addresses.
- RFC 1918, *Address Allocation for Private Internets* , has set aside the following IPv4 address space for private use:
  - **Class A network:** 10.0.0.0 to 10.255.255.255
  - **Class B network:** 172.16.0.0 to 172.31.255.255
  - **Class C network:** 192.168.0.0 to 192.168.255.255

NAT

NAT používa pojem *inside* and *outside*

- *Inside* znamená interne v danej sieti
- *Outside* znamená mimo (externe) danú sieť

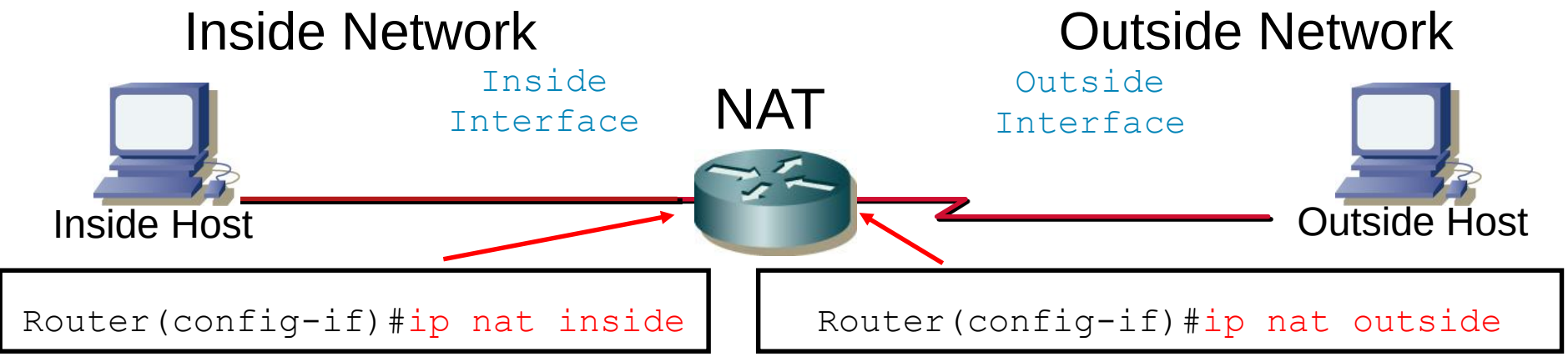
- Nat hovorí o nasledujúcich typoch adries
  - **Inside Local Addresses**
    - IP adresa pridelená IP zariadeniu vo vnútri siete. Adresa je typicky privátna podľa RFC 1918.
  - **Inside Global Address**
    - Platná verejná IP adresa, pridelená ISP.
    - Na túto adresu bude prekladaná privátna zdrojová adresa v odchodzom pakete ak ten opúšťa vnútornú sieť cez NAT.
  - **Outside Global Address**
    - Platná verejná IP adresa, pridelená koncovému IP zariadeniu tak ako to vidí odosielateľ z vnútornej siete.
  - **Outside Local Address**
    - Lokálna IP adresa pridelená zariadeniu vo vonkajšej sieti. Typicky ak táto sieť nepoužíva tiež NAT je zhodná z Outside Global Address.



Typy NAT

- **Statické mapovanie**
  - Tzv. „one-to-one mapping“
  - Spárovanie prekladu jednej privátnej adresy (inside local) na jednu verejnú adresu (inside global)
  - Výhodné, priam potrebné ak potrebujem zabezpečiť prístup na stanicu (napr. HTTP server) za NAT z Internetu
- **Dynamické mapovanie**
  - NAT má dostupný rozsah verejných adries
    - Tzv. IP address pool
  - NAT riadi preklad prideľovaním neobsadených verejných IP adries z rozsahu podľa príchodzích požiadaviek z vnútra siete
  - Je potrebné zabezpečiť dostatok adries v pool-e
- **Port Address Translation (PAT) (NAT overloading)**
  - Používaný ak je málo verejných IP adries
  - PAT mapuje viaceré IP adresy na jednu verejnú/viaceré IP adresu, kde sa prebiehajúce komunikácie rozlišujú číslom portu (16 bit)

Zadefinovanie Inside/Outside rozhraní



- Pri NAT sa definujú vždy!!!!
- Rozhranie border routra pri NAT môže byť
  - Inside (vnútorné s privátnou adresáciou)
  - alebo Outside (s verejnou adresáciou)
- NAT preklad nastáva:
  - Len pri prechode paketu z inside na outside a naopak
  - Nikdy medzi rozhraniami toho istého typu, alebo nezadefinovanými

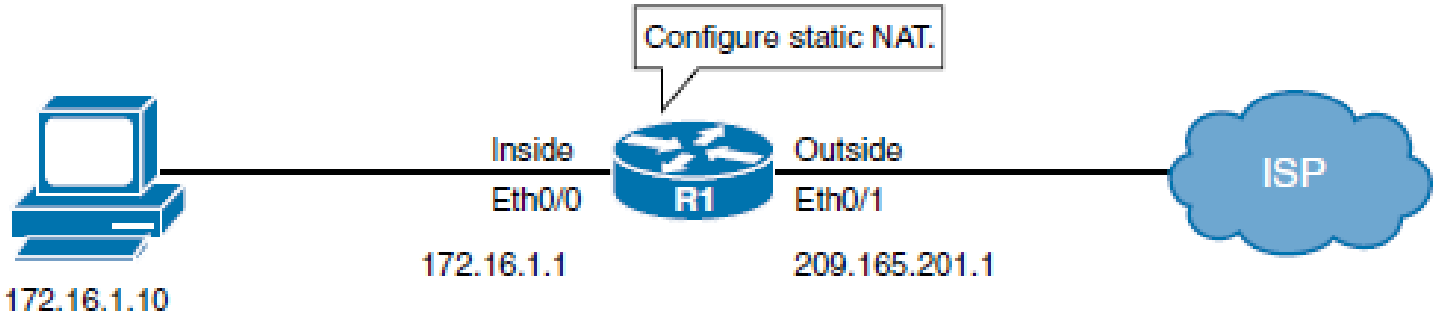
Konfigurácia Static NAT

- Príkazom zadám priamo do konfigurácie mapovanie, ktoré ostáva permanentne uložené v mapovacej prekladovej tabuľke NAT-u
  - Aj po reštarte, za predpokladu copy run start

```
Router(config)# ip nat inside source static INSIDE_LOCAL INSIDE_GLOBAL
```

Parameter	Description
local-ip	The inside local IPv4 address assigned to a host on the inside network.
global-ip	The inside global IPv4 address of an inside host as it appears to the outside world

Konfigurácia Static NAT - Príklad




```
Router(config)# interface Ethernet 0/1
Router(config-if)# ip address 209.165.201.1 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# ip nat inside source static 172.16.1.10 209.165.201.5
```

Konfigurácia dynamického NAT prekladu

- Pozostáva z:
  - Definovanie Inside/outside rohraní
  - Definovanie rozsahu verejných adries (tzv. NAT pool), z ktorých bude pri preklade vyberané

```
Router(config)#ip nat pool MENO_POOLU START-IP END-IP netmask MASKA
```

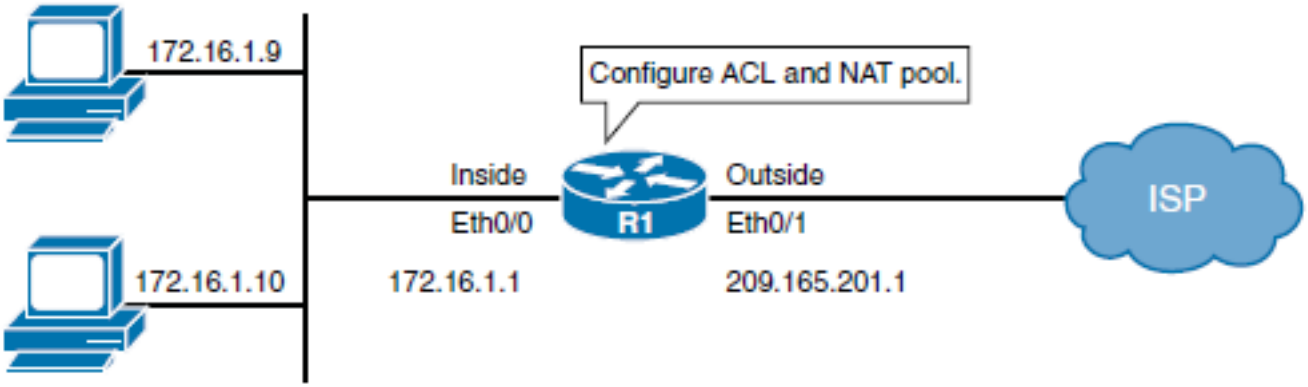
  - Zadefinovania IP adries cez ACL, pre ktoré NAT bude vykonávať preklad

```
Router(config)#access-list CISLO-ACL-LISTU permit SOURCE WILDCARD-MASK
```

  - Spojenie ACL a daného pool-u do funkčného dynamického NAT

```
Router(config)#ip nat inside source list CISLO-ACL-LISTU pool MENO-POOLU
```

Konfigurácia dynamického NAT - príklad




```
Router(config)# access-list 1 permit 172.16.1.0 0.0.0.255
Router(config)# ip nat pool NAT-POOL 209.165.201.5 209.165.201.10
  netmask 255.255.255.240
Router(config)# interface Ethernet 0/1
Router(config-if)# ip address 209.165.201.1 255.255.255.240
Router(config-if)# ip nat outside
Router(config-if)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)#exit
Router(config)# ip nat inside source list 1 pool NAT-POOL
```

Preťažovanie rozhrania

- Pozostáva z:
  - Definovanie Inside / outside
  - Zadefinovania IP adries cez ACL, pre ktoré NAT bude vykonávať preklad

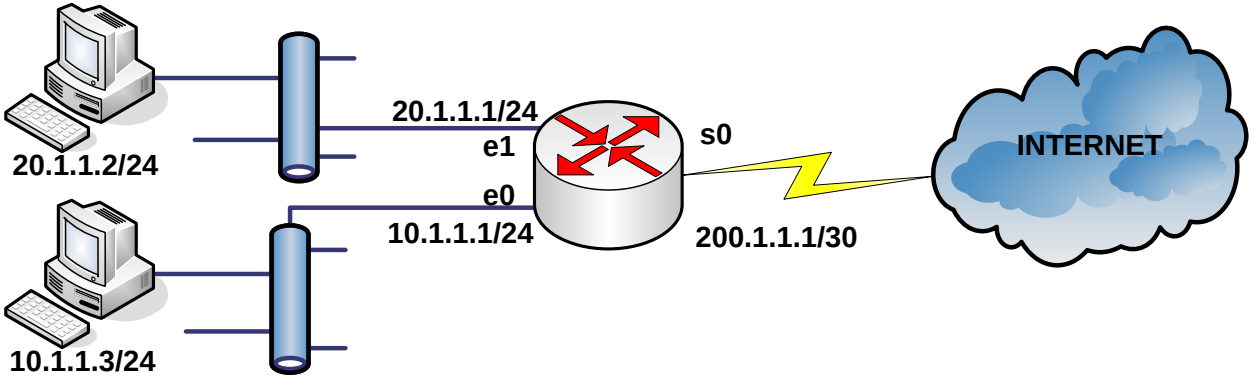
```
Router(config)#access-list CISLO-ACL-LISTU permit SOURCE WILDCARD-MASK
```

  - Určenie rozhrania, ktoré sa „preťaží“

```
Router(config)# ip nat inside source list CISLO-ACL-LISTU interface INT overload
```

Konfigurácia PAT

Preťaženie rozhrania – príklad




```
Gw(config)#int ethernet 0
Gw(config-if)#ip address 10.1.1.1 255.255.255.0
Gw(config-if)#ip nat inside
Gw(config)#int ethernet 1
Gw(config-if)#ip address 20.1.1.1 255.255.255.0
Gw(config-if)#ip nat inside
Gw(config)#int serial 0
Gw(config-if)#ip address 200.1.1.1 255.255.255.252
Gw(config-if)#ip nat outside
Gw(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Gw(config)#access-list 1 permit 20.1.1.0 0.0.0.255
Gw(config)#ip nat inside source list 1 interface serial 1/0 overload
```

Preťaženie adresného rozsahu

- Pozostáva:
  - Zadefinovanie IP adries cez ACL, pre ktoré PAT bude vykonávať preklad

```
Router(config)#access-list CISLO-ACL-LISTU permit SOURCE WILDCARD-MASK
```

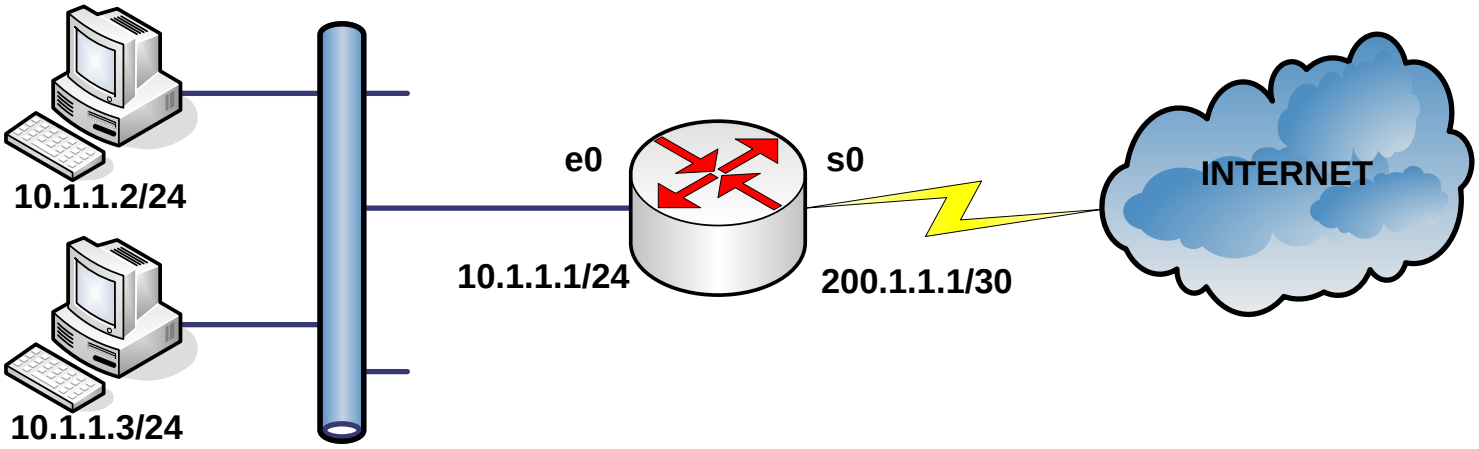
  - Zadefinovanie rozsahu verejných adries (tzv. NAT pool), z ktorých bude pri preklade vyberané

```
Router(config)#ip nat pool MENO_POOLU START-IP END-IP netmask MASKA
```

  - Spojenie ACL a daného pool-u do funkčného dynamického PAT

```
Router(config)# ip nat inside source list CISLO-ACL-LISTU pool MENU_POOLU overload
```

Preťaženie rozsahu adries - príklad




```
Gw(config)#int ethernet 0
Gw(config-if)#ip address 10.1.1.1 255.255.255.0
Gw(config-if)#ip nat inside
Gw(config-if)#no shut
Gw(config-if)#exit
Gw(config)#int serial 0
Gw(config-if)#ip address 200.1.1.1 255.255.255.252
Gw(config-if)#ip nat outside
Gw(config-if)#no shut
Gw(config-if)#exit
Gw(config)#ip nat pool MOJ_ROZSAH 211.2.2.8 211.2.2.10 netmask 255.255.255.252
Gw(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Gw(config)#ip nat inside source list 1 pool MOJ_ROZSAH overload
```

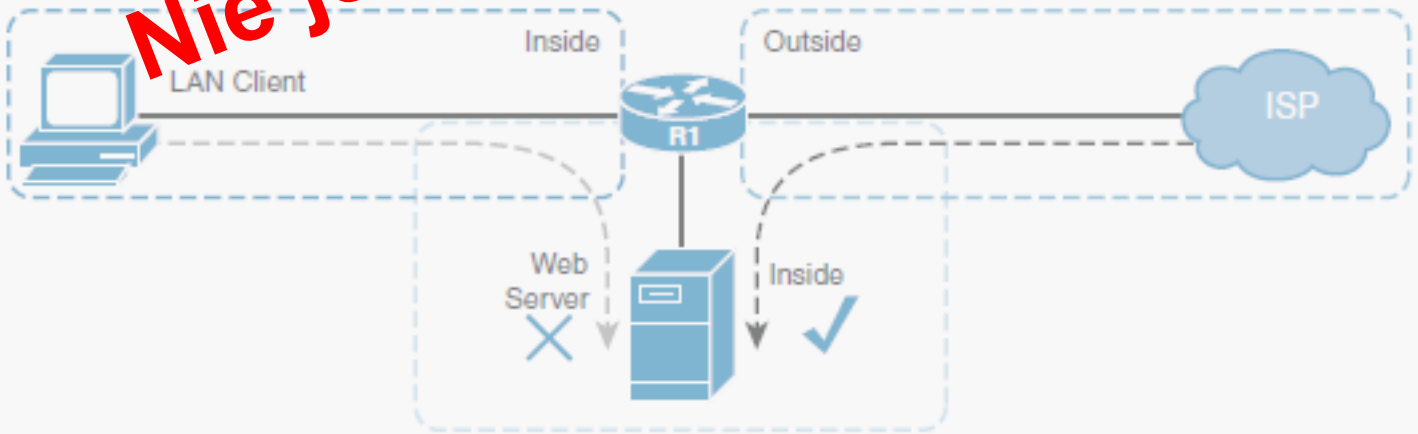
Limitations of NAT

- **End-to-end visibility issues:**
  - Many applications depend on end-to-end functionality, with unmodified packets being forwarded from source to destination. By changing end-to-end addresses, NAT effectively blocks such applications.
- **Tunneling becomes more complex:**
  - Using NAT can complicate tunneling protocols, such as IPsec, because NAT modifies the values in the headers and thus interferes with the integrity checks done by IPsec and other tunneling protocols.

Limitations of NAT

- **In certain topologies, standard NAT may not work correctly**
  - R1 router is configured to perform PAT for the LAN clients and static NAT for the web server.
  - When a client on the Internet wants to access the web server, it gets the server's public IP address from the DNS. The router statically translates the server's public IP address to its inside local address, and forwards packets to the server.
  - When a client on the LAN tries to access the server, it similarly gets the same public IP address for the server from DNS, and tries to access the server. However, attempts to connect to the server will fail because of how NAT operates.
  - When packets go from inside to outside, they are first routed and then translated; the packets from the LAN client are routed to the outside interface and the LAN client's address is translated by PAT. When packets travel from outside to inside, they are translated and routed. In this case however, the packets from the LAN client do not come in the router's outside interface; therefore, they are never translated so they are never routed back to the interface where the server is located.
  - The result is that the LAN client cannot connect to the web server.

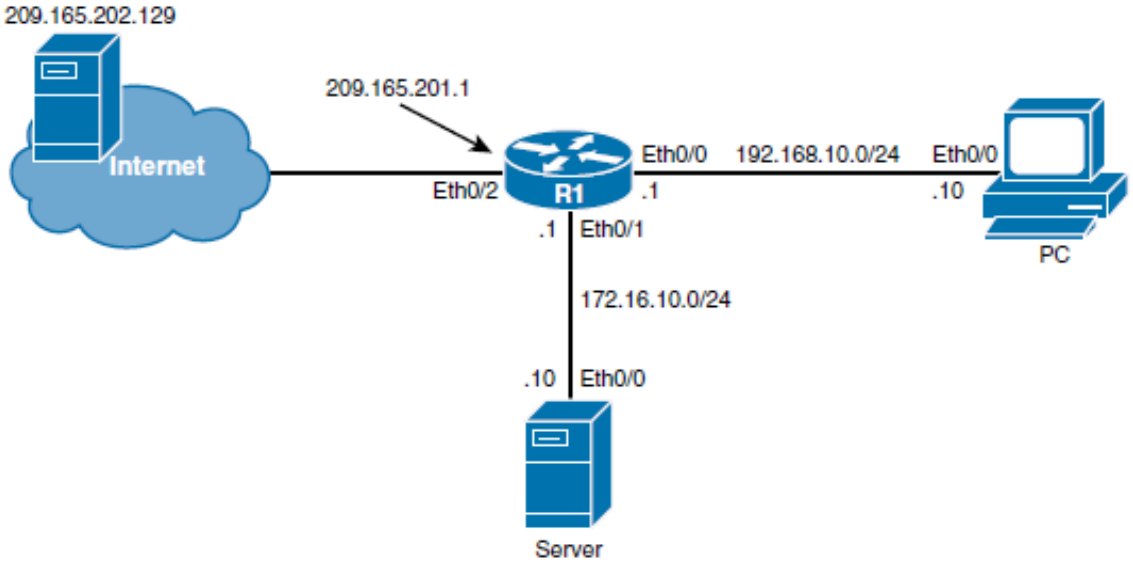
Nie je celkom pravda = DNS views



NAT Virtual Interface

- NAT virtual interface (NVI),
  - Uvedené v Cisco IOS Software Release 12.3(14)T
  - Odstraňuje potrebu konfigurovať rozhranie ako inside or outside.
- Pracuje trochu inak ako klasické NAT
  - Klasické NAT vykoná routing, a ak paket ide z Inside na Outside vykoná NAT-ovanie
  - V opačnom smere reverzne
- NVI vykonáva
  - routing, preklad, a znovu routing
  - Routing je vykonaný teda 2x
    - Pred a po preklade NAT virtual interface (NVI)
- Proces je obojsmerne symetrický
  - Je jedno ktorým smerom paket tečie
- POZN. K slajdu predtým
  - Because of the added routing step, packets can flow, in classic NAT terms, from an inside to an inside interface; as described in the previous section, this scenario fails if classic NAT is used.

Konfigurácia NAT Virtual Interface




```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# ip nat pool TEST1 209.165.201.5 209.165.201.10 prefix-length 27
R1(config)# ip nat source list 10 pool TEST1
R1(config)# ip nat source static 172.16.10.10 209.165.201.2
```

```
R1(config)# interface ethernet 0/0
R1(config-if)# ip nat enable
R1(config-if)# interface ethernet 0/1
R1(config-if)# ip nat enable
R1(config-if)# interface ethernet 0/2
R1(config-if)# ip nat enable
```

NVI Interface

```
R1# show ip interface brief
Interface        IP-Address      OK?  Method  Status                Protocol
Ethernet0/0      192.168.10.1    YES  manual  up                    up
Ethernet0/1      172.16.10.1     YES  manual  up                    up
Ethernet0/2      209.165.201.1   YES  manual  up                    up
Ethernet0/3      unassigned      YES  NVRAM   administratively down down
NVI0             192.168.10.1    YES  unset   up                    up
```

- Keď paket vstúpi do NAT smerovača cez rozhranie s povoleným NAT (NAT enabled)
  - Je porovnaný voči NAT tabuľke
  - Ak je zhoda, je smerovaný na NVI0
    - Tu sa vykoná preklad
  - Po preklade je paket vrátený späť a urobí sa znovu smerovanie na dané výstupné rozhranie
- POZN:
  - NVI rozhranie má pridelenú IPv4 adresu, ktorá je potrebná pre operácie vnútri IOS.
  - Je zvyčajne kopírovaná z prvého rozhrania na ktorom je povolené NAT
  - Nemá vplyv na činnosť NAT

Overenie - show ip nat nvi translations

```
R1# show ip nat nvi translations
Pro Source global       Source local        Destin  local        Destin  global
icmp 209.165.201.2:0    172.16.10.10:0      209.165.202.129:0    209.165.202.129:0
--- 209.165.201.2       172.16.10.10        ---                  ---
icmp 209.165.201.5:0    192.168.10.10:0     209.165.202.129:0    209.165.202.129:0
icmp 209.165.201.5:1    192.168.10.10:1     172.16.10.10:1       172.16.10.10:1
icmp 209.165.201.5:2    192.168.10.10:2     209.165.201.2:2      172.16.10.10:2
--- 209.165.201.5       192.168.10.10       ---                  ---
```

```
R1# show ip nat translations
Pro Inside global    Inside local     Outside local    Outside global
```

show ip nat nvi statistics

```
R1# show ip nat nvi statistics
Total active translations: 4 (1 static, 3 dynamic; 2 extended)
NAT Enabled interfaces:
  Ethernet0/0, Ethernet0/1, Ethernet0/2
Hits: 34  Misses: 4
CEF Translated packets: 10, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Source [Id: 3] access-list 10 pool TEST1 refcount 2
 pool TEST1: netmask 255.255.255.224
        start 209.165.201.5 end 209.165.201.10
        type generic, total addresses 6, allocated 1 (16%), misses 0
```

Založenie Single-Homed IPv6 Internet konektivity

Budovanie Single-Homed IPv6 Internet konektivity

- Popíšeme:
  - Spôsoby ako môže router získať IPv6 adresu
  - Vysvetlenie operácii DHCP pre IPv6 (DHCPv6)
  - Konfigurácia DHCPv6 ako server a relay agent
  - Použitie NAT pre IPv6
  - Konfigurácia IPv6 ACLs

Získanie IPv6 adresy od poskytovateľa

Je možné nasledujúcimi spôsobmi:

- Manual nastavenie pridelenej IPv6 adresy
- Stateless address autoconfiguration (SLAAC)
- Stateless DHCPv6
- Stateful DHCPv6
- DHCPv6 prefix delegation (DHCPv6-PD)

Manuálna konfigurácia IPv6 adresy

- Konfiguráciu IPv6 smerovania na smerovači je potrebné najprv aktivovať príkazom

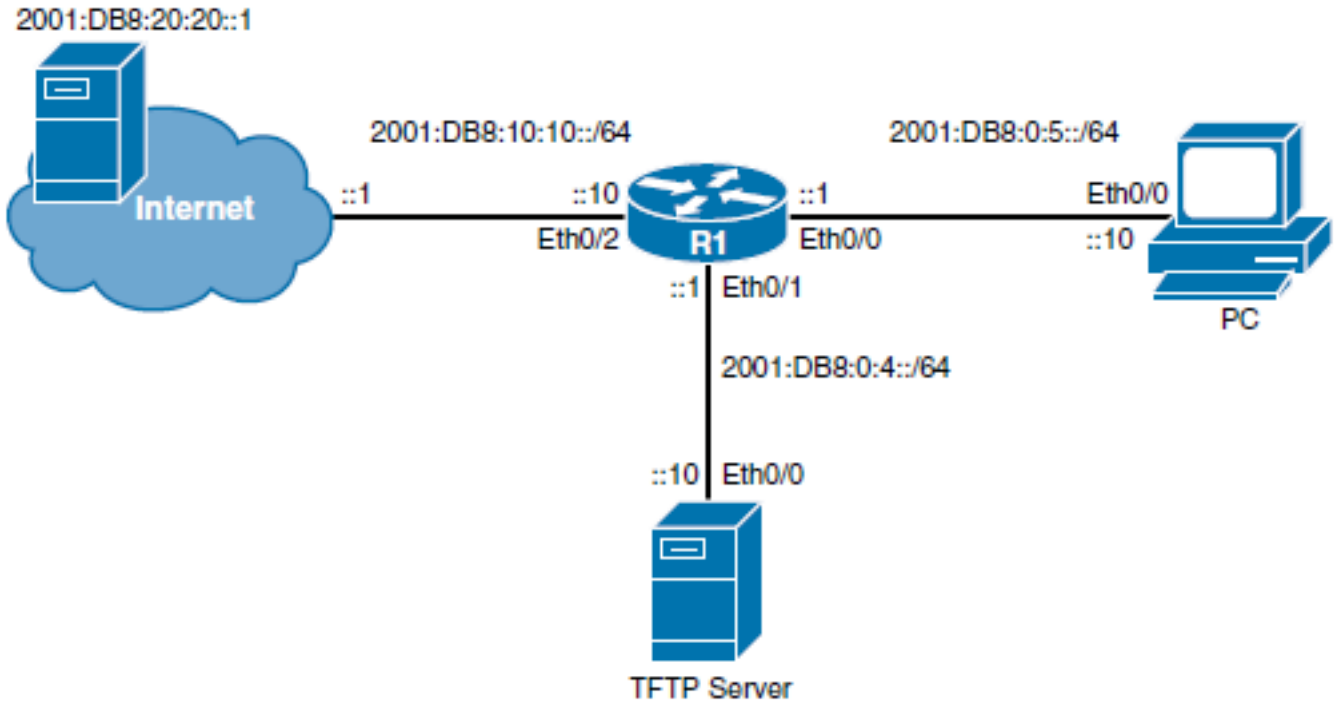
```
Router(config)#
ipv6 unicast-routing
```

- IPv6 sa konfiguruje veľmi podobne ako IPv4
  - Vo všetkých známych príkazoch sa píše „ipv6“ namiesto „ip“
  - Platí pre konfiguráciu adries či statických ciest
  - Aj overovanie

```
Router(config)# ipv6 route 2000::/3 2001:4118:300:122::1
Router(config)# interface fa0/0
Router(config-if)# ipv6 address 2001:4118:300:123::1/64
```

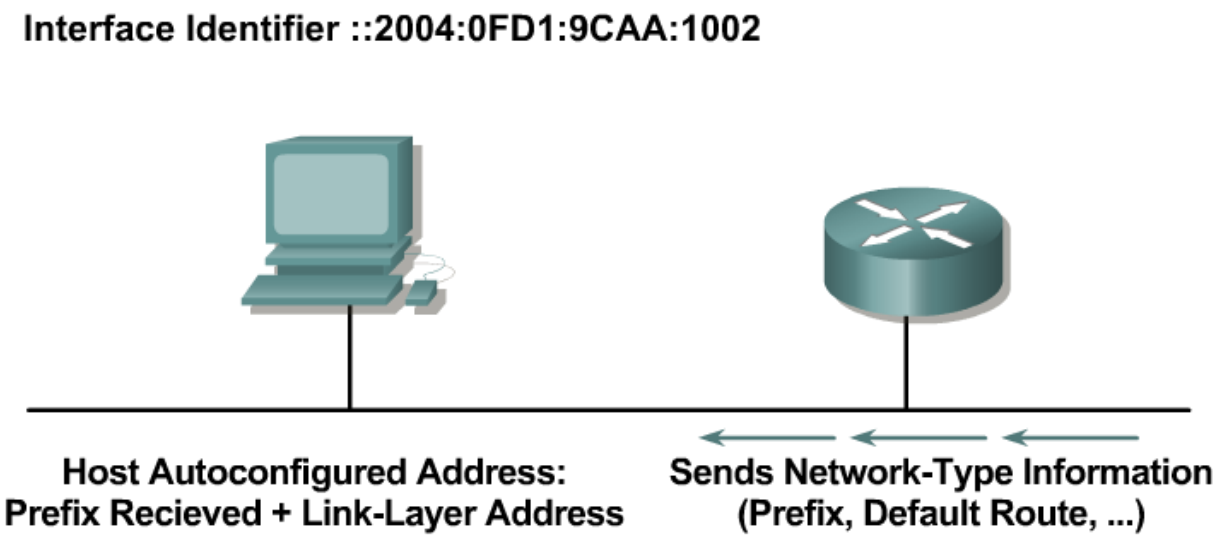
```
! Static LL
! Zvycajne auto po povoleni IPv6 ako EUI-64
Router(config-if)# ipv6 address FE80::1 link-local
```

Manuálna konfigurácia IPv6 adresy - príklad



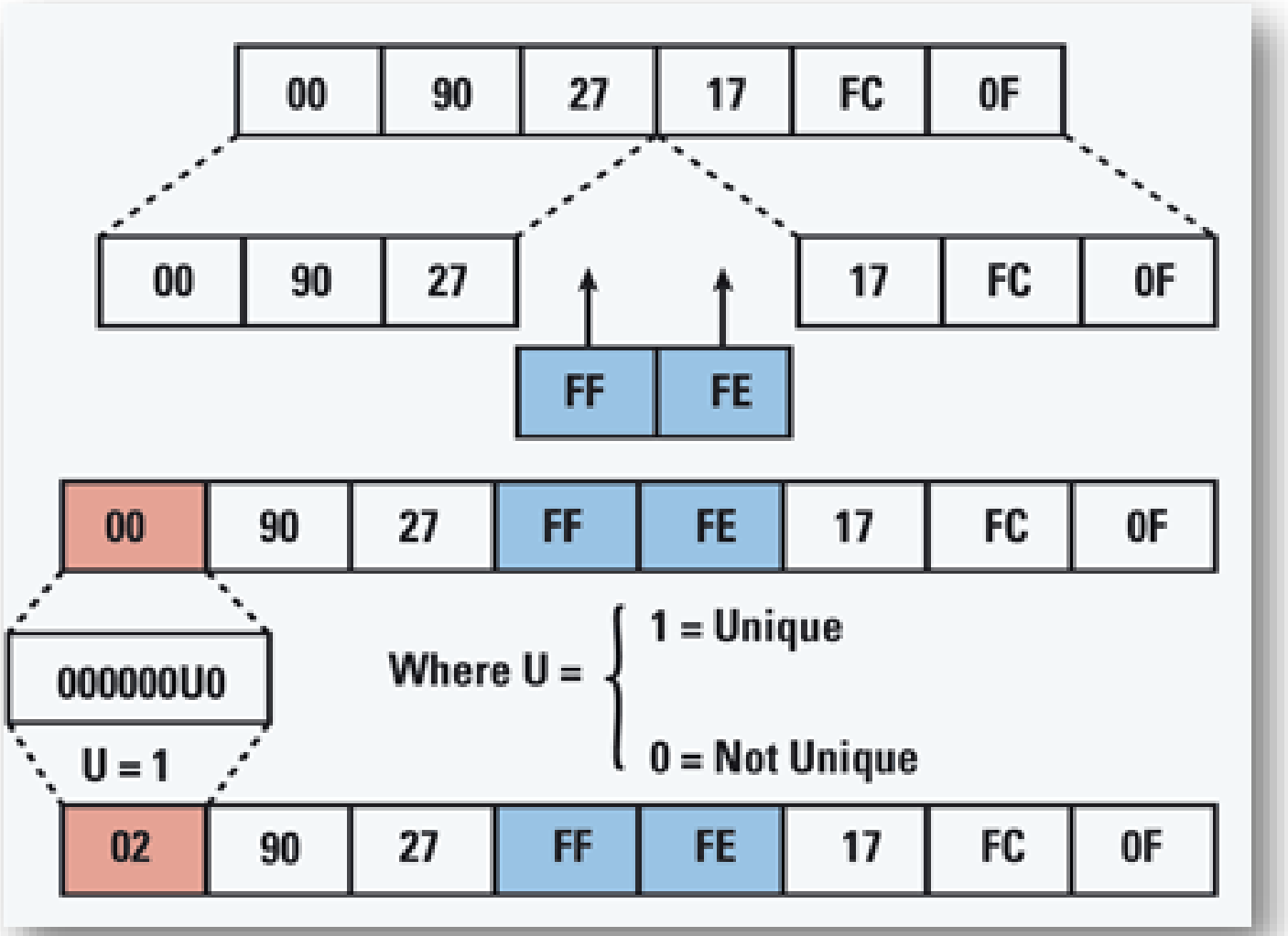

```
R1(config)# ipv6 unicast-routing
R1(config)# interface Ethernet 0/2
R1(config-if)# ipv6 address 2001:DB8:10:10::10/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ipv6 route ::/0 2001:DB8:10:10::1
```

Bezstavová konfigurácia (Stateless Autoconfiguration)

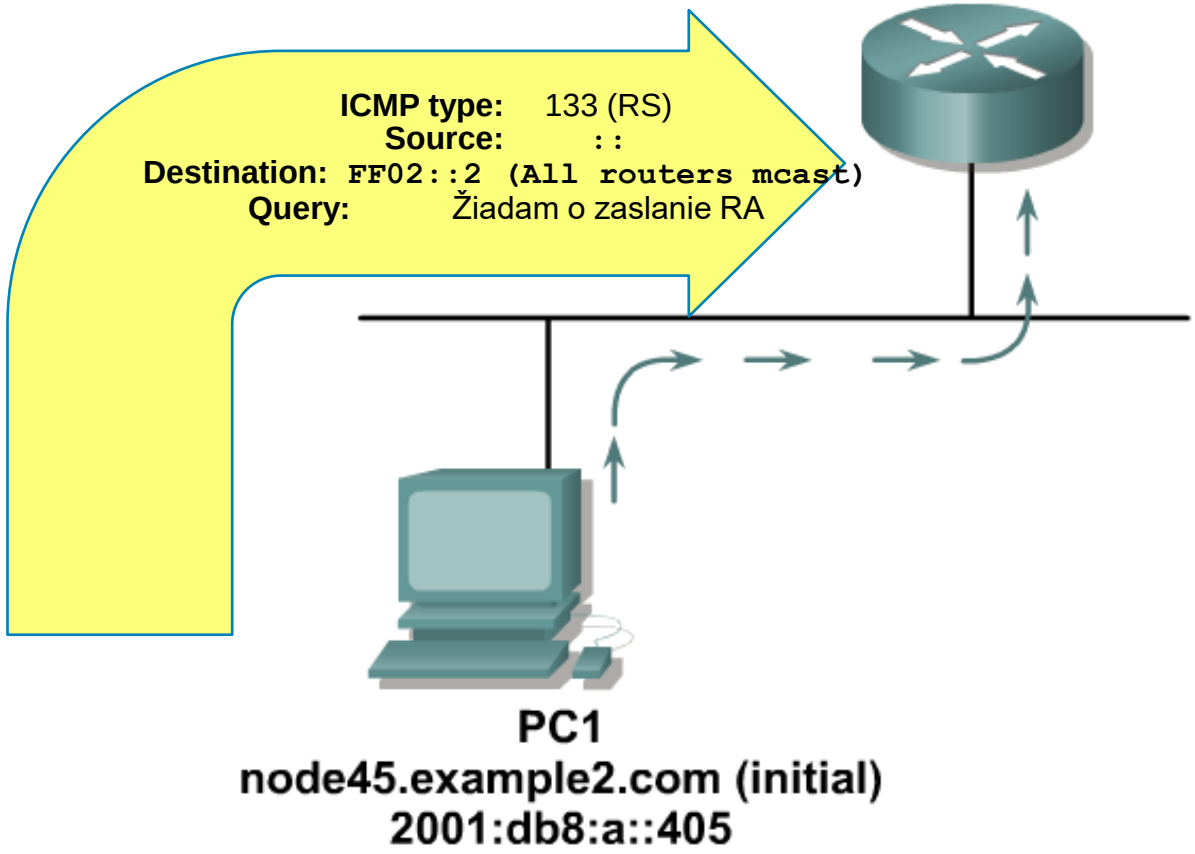


- Každá IPv6 stanica si dokáže sama prideliť IPv6 adresu
  - tak, že pripojí svoj 64-bitový Interface ID (EUI 64) k prefixu siete, ktorý prijala od routera v RA správe
  - Overí adresu cez DAD
- Smerovač za týmto účelom posiela rozhraním informácie všetkým uzlom na sieti
  - tzv. ICMP router advertisement správy, RA
  - RA je posielané periodicky, ale uzol si zaslanie môže vynútiť generovaním správy RS

Konverzia MAC adresy na IEEE EUI-64

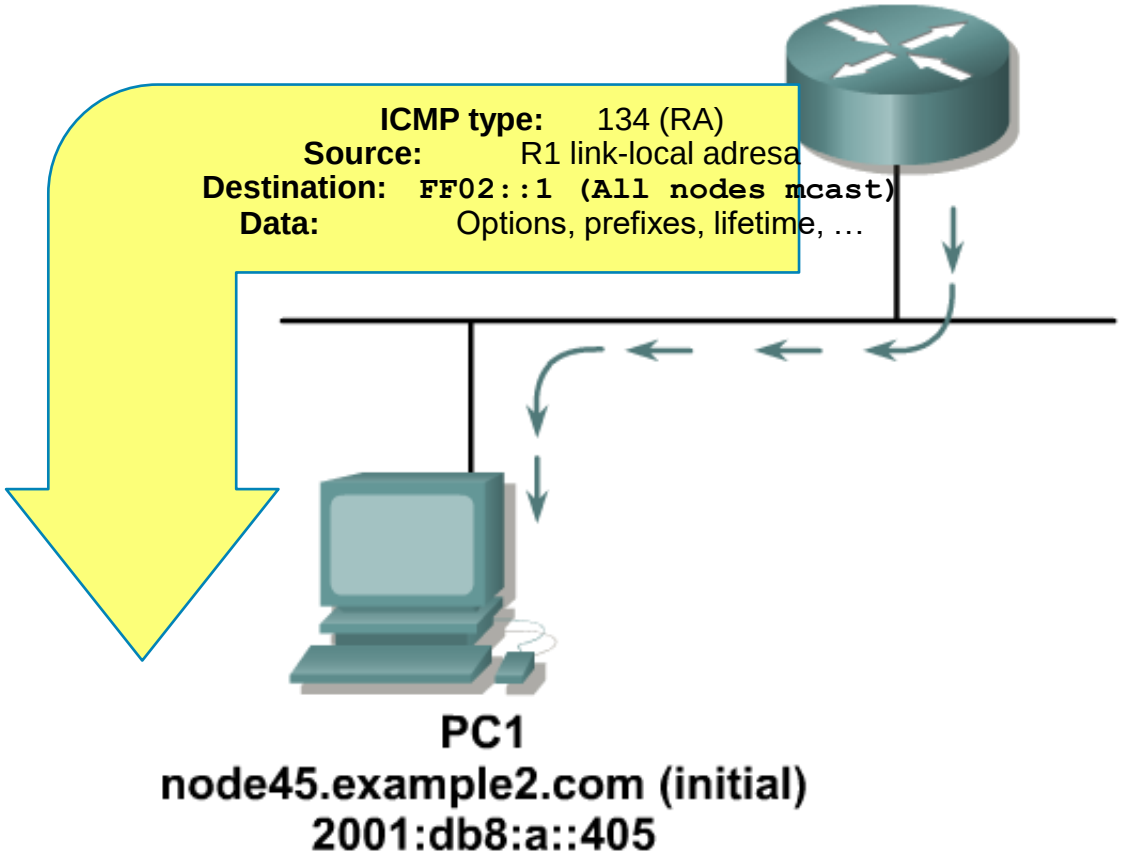


Postup bezstavovej konfigurácie adresy



- Fáza 1: PC odošle správu „router solicitation (RS)“ a vyžiada si sieťový prefix pre bezstavovú konfiguráciu

Postup bezstavovej konfigurácie adresy



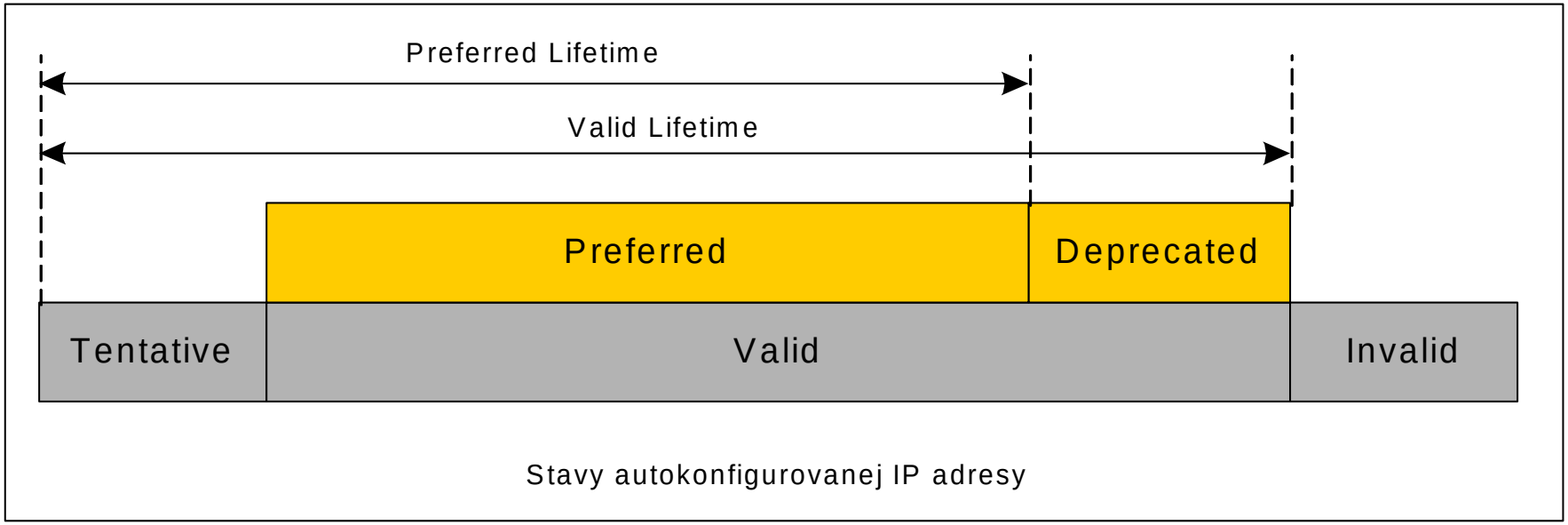
- Fáza 2: Router odpovedá správou Router Advertisement, v ktorej uvedie okrem iných údajov aj prefix lokálnej siete

Autokonfigurované adresy

- Stavy automaticky nastavenej adresy:
  - **Tentative** (neoverená, pokusná)
    - V procese preverovania unikátnosti (Duplicate Address Detection)
    - Unicast komunikácia je zakázaná
    - Multicast komunikácia – len správy Neighbor Advertisement
  - **Valid** (platná)
    - Unikátnosť adresy bola potrvrdená
    - Adresu je možné používať
    - Stav Valid obsahuje v sebe ďalšie 2 stavy
      - **Preferred** (normálny stav) – adresa je platná
      - **Deprecated** (neschválená) – adresa je platná, ale je zbavená schopnosti nadväzovať nové spojenia
        - existujúca komunikácia môže prebiehať ďalej
  - **Invalid** (neplatná)
    - Do tohto stavu sa adresa dostane po uplynutí časovača Valid Lifetime
    - Adresa v tomto stave nie je použiteľná

Stavy automatickej IP adresy

- Autokonfigurovaná adresa prechádza týmito stavmi cyklicky
- Trvanie stavov získa zo správy Router Advertisement
- Autokonfigurované adresy obvykle patria na koncové stanice, smerovače ich spravidla nevyužívajú



Stavy autokonfigurovanej IP adresy

Bezstavová autokonfigurácia

```
Router(config-if)#
ipv6 address autoconfig [default]
```

- Adresa je pridelená na základe prefixu prijatého v RA
- **default**:
  - inštalácia default route cez tento smerovač
  - Povolené zadať len na jednom rozhraní
- Poznámka k správaniu sa IPv6 smerovača
  - Smerovač s **ipv6 unicast-routing** generuje ICMP RA, negenruje ICMP RS správy
  - Smerovač s **ipv6 address autoconfig** a bez **ipv6 unicast-routing** generuje ICMP RS, negeneruje ICMP RA

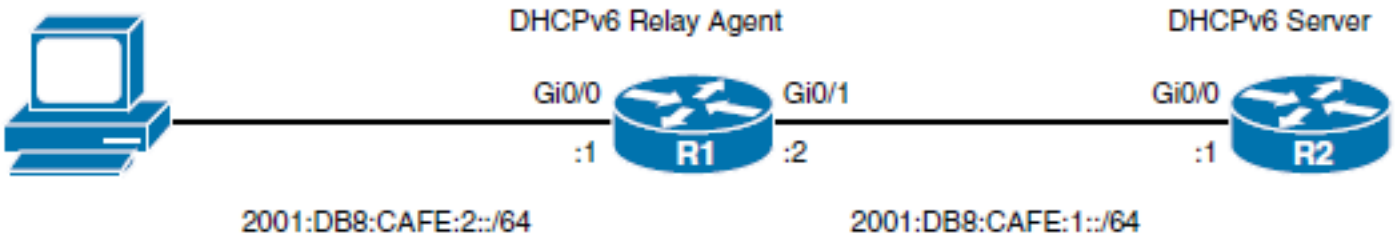
DHCPv6 Operation

- V IPv6 je indikácia použitia DHCPv6 riešená v súčinnosti s SLAAC
- Sú dva spôsoby nasadenia DHCPv6:
  - **Stateless:**
    - Poskytuje dodatočne parametre k údajom získaným cez SLAAC
  - **Stateful:**
    - Podobné k DHCP pre IPv4 (DHCPv4)

Stateless DCHPv6

- Stateless DHCPv6 pracuje v súčinnosti so SLAAC
  - SLACC
    - Cez SLAAC IPv6 host získa informáciu k vytvoreniu jeho IPv6 adresy ako aj adresu default router
      - Obsiahnuté v IMCP RA (prefix, prefix length, def. router)
    - Zároveň je mu naznačené cez príznak *other configuration* flag bit, že ďalšie údaje má získať cez DHCPv6
      - Napr. DNS, NTP apod
  - DHCPv6
    - IPv6 host následne kontaktuje DHCPv6 server aby získal ďalšie parametre
    - Server teda nepridelʼuje IPv6 adresy, a nepotrebuje si ani o ničom viesť stavové informácie ➔ stateless

Konfigurácia Stateless DCHPv6



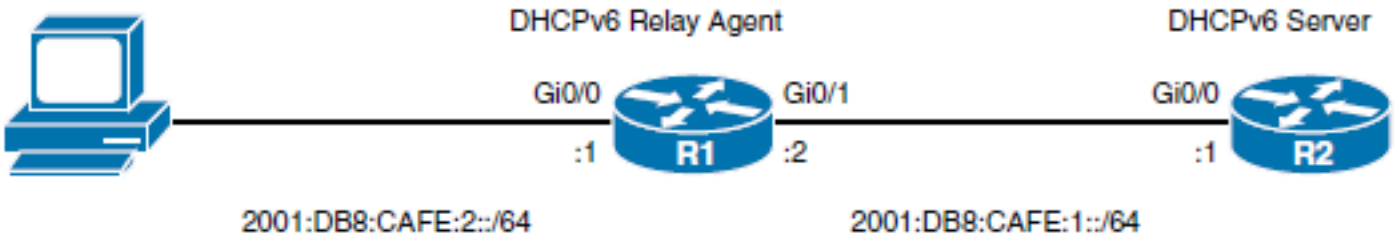

```
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# ipv6 dhcp relay destination 2001:DB8:CAFE:1::1

R2(config)# ipv6 dhcp pool IPV6-STATELESS
R2(config-dhcpv6)# dns-server 2001:DB8:CAFE:1::99
R2(config-dhcpv6)# domain-name www.example.com
R2(config)# interface gigabitEthernet 0/0
R2(config-if)# ipv6 dhcp server IPV6-STATELESS
```

Stateful DHCPv6

- SLAAC
  - Poskytne stanici adresu Default gateway
  - Avšak cez ICMP RA flag *managed address configuration* povie IPv6 stanici, že všetko ďalšie získa cez DHCPv6
    - Flag informuje aby stanica ignorovala údaje z ICMP RA
- DHCPv6
  - Manažuje pridelenie všetkých parametrov vrátane IPv6 adresy
  - Vedie si záznamy o zápožičkách
    - Tak ako v DHCPv4

Konfigurácia Stateful DHCPv6




```
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# ipv6 dhcp relay destination 2001:DB8:CAFE:1::1

R2(config)# ipv6 dhcp pool IPV6-STATEFUL
R2(config-dhcpv6)# address prefix 2001:DB8:CAFE:2::/64
R2(config-dhcpv6)# dns-server 2001:DB8:CAFE:1::99
R2(config-dhcpv6)# domain-name www.example.com
R2(config)# interface gigabitEthernet 0/0
R2(config-if)# ipv6 dhcp server IPV6-STATEFUL
```

Činnosť DHCPv6

- The client sends a **SOLICIT** message to find a DHCPv6 server and request assignment of addresses and other configuration information.
- This message is sent to the *all-DHCP-agents* multicast address (FF02::1:2) with link-local scope
- Any DHCPv6 servers that can meet the client's requirement respond to the client with an **ADVERTISE** message.
- The client chooses one of the servers and sends a **REQUEST** message to it, asking it to confirm the addresses and other information that were advertised.
- The server responds with a **REPLY** message that contains the confirmed addresses and configuration information.
- Like with DHCPv4, a DHCPv6 client renews its lease after a period of time by sending a RENEW message.
- By default, the four-message exchange is used; when the **rapid-commit** option is enabled by both the client and server, the two-message exchange is used (SOLICIT-REPLY).

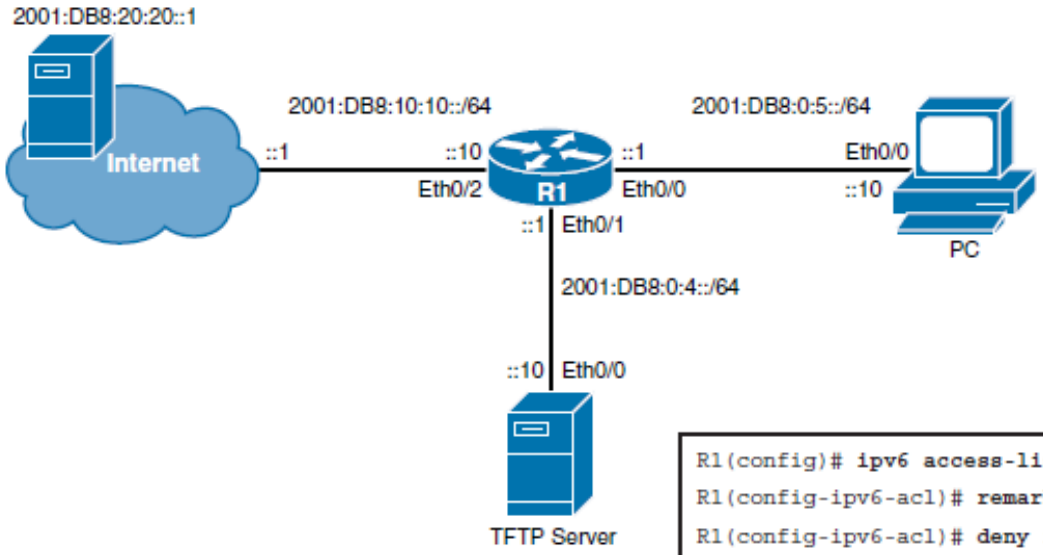
NAT pre IPv6

- NAT v IPv6 má iné nasadenie ako v IPv4
  - IPv4 NAT Preklad IPv4 private adries na IPv6 public adresy
  - IPv6 nemá pojem private adresy
  - NAT tu však existuje
- NAT v IPv6
  - NAT64
    - IPv4 to IPv6 migračná technika
    - NAT64 vykonáva dvojitý preklad aj zdrojovej aj cieľovej adresy
      - Avšak z IPv6 do Ipv4 a naopak
  - NPTv6
    - NPTv6 popisované v RFC 6296, *IPv6-to-IPv6 Network Prefix Translation*
      - Stále len experimental RFC, nie štandard
    - Rieši IPv6 one-to-one stateless preklad;
    - Jedna IPv6 adresa z inside siete (napr. LAN organizácie)
    - Preložená na jednu IPv6 adresu z outside siete (IPv6 Internet)

IPv6 ACLs

- IPv6 má len named ACL, nie číslované ako v IPv4
- Navyše v IPv6 ACL sú na konci **tri** implicitné pravidlá:
  - **`permit icmp any any nd-na`**
  - **`permit icmp any any nd-ns`**
  - **`deny ipv6 any any`**
- Logging
  - Napr. **deny ipv6 any any log**.
- Pozor:
  - explicitné **deny** prepíše všetky tri implicitné pravidlá

Konfigurácia IPv6 ACL - príklad




```
R1(config)# ipv6 access-list SECURE_HOSTS
R1(config-ipv6-acl)# remark DENY PING TO TFTP SERVER
R1(config-ipv6-acl)# deny icmp any host 2001:DB8:0:4::10 echo-request
R1(config-ipv6-acl)# remark DENY TELNET TO TFTP SERVER
R1(config-ipv6-acl)# deny tcp any host 2001:DB8:0:4::10 eq telnet
R1(config-ipv6-acl)# remark ALLOW TFTP ONLY TO TFTP SERVER
R1(config-ipv6-acl)# permit udp any host 2001:DB8:0:4::10 eq tftp
R1(config-ipv6-acl)# deny udp any any eq tftp
R1(config-ipv6-acl)# remark ALLOW ALL OTHER TRAFFIC
R1(config-ipv6-acl)# permit ipv6 any any
```

```
R1(config)# interface Ethernet 0/2
R1(config-if)# ipv6 traffic-filter SECURE_HOSTS in
```

Overenie IPv6 ACLs

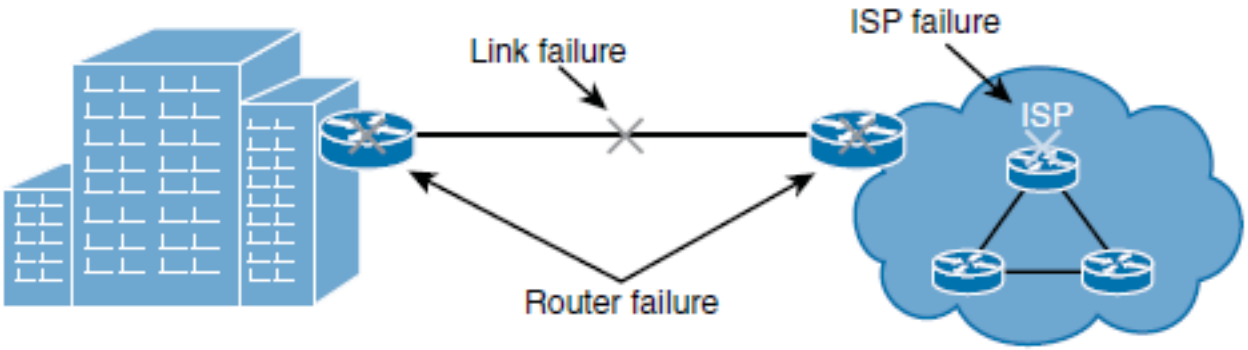
```
R1# show ipv6 access-list
IPv6 access list SECURE_HOSTS
    deny icmp any host 2001:DB8:0:4::10 echo-request (5 matches) sequence 20
    deny tcp any host 2001:DB8:0:4::10 eq telnet (1 match) sequence 40
    permit udp any host 2001:DB8:0:4::10 eq tftp (4 matches) sequence 60
    deny udp any any eq tftp (6 matches) sequence 70
    permit ipv6 any any (44 matches) sequence 90
```

Improving Internet Connectivity Resilience

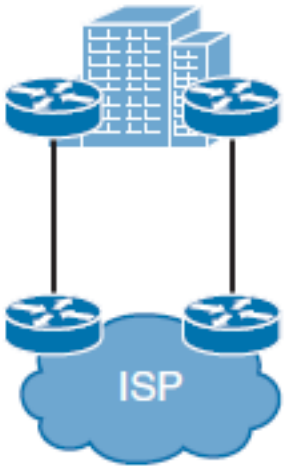
Improving Internet Connectivity Resilience

- Describe the disadvantages of single-homed Internet connectivity
- Describe dual-homed Internet connectivity
- Describe multihomed Internet connectivity

Drawbacks of a Single-Homed Internet Connectivity



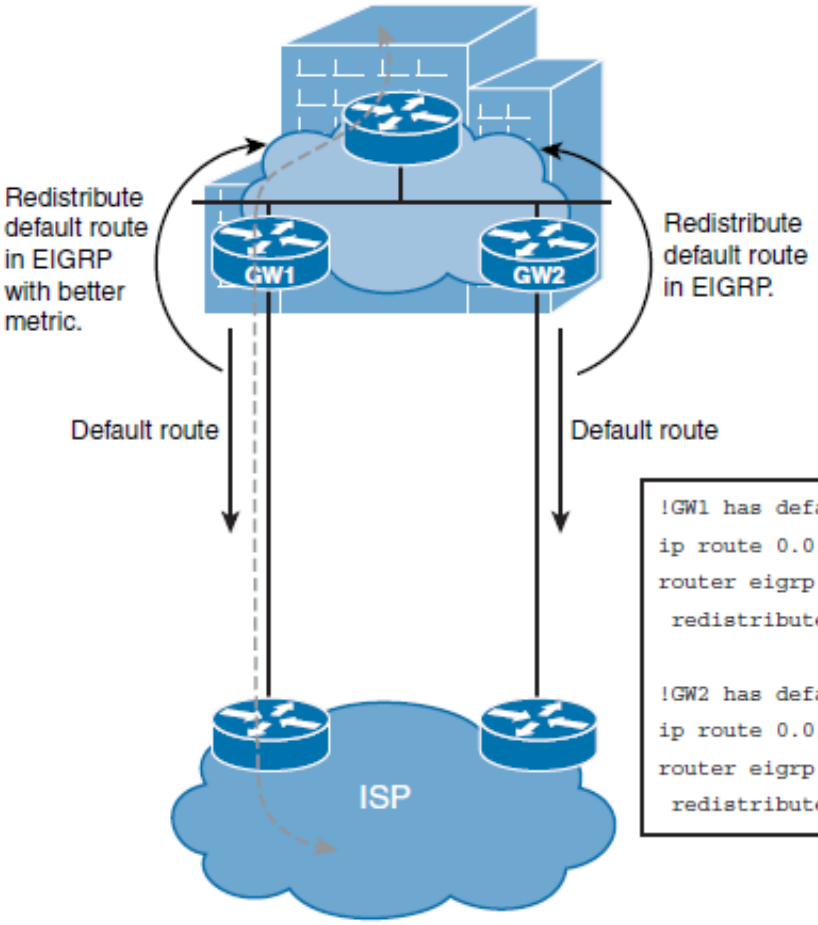
Dual-Homed Internet Connectivity



Configuring Best Path for Dual-Homed Internet Connectivity

- In dual-homed networks, one link is usually used as a primary link. In case of primary link failure, the second (backup) link is used for traffic forwarding.
- Either static routing toward the ISP or BGP with the ISP are commonly used to route outbound traffic.
- Internet routing information must also be available to the organization's internal routing protocol. In simple networks, static routes with different ADs (called floating static routes) can be used.
- Alternatively, you can redistribute a default route or a subset of Internet routes into your internal routing protocol.
- First-hop redundancy protocols (FHRPs) can also be used to properly route packets to the appropriate Internet gateway.

Dual-Homed EIGRP and Static Example

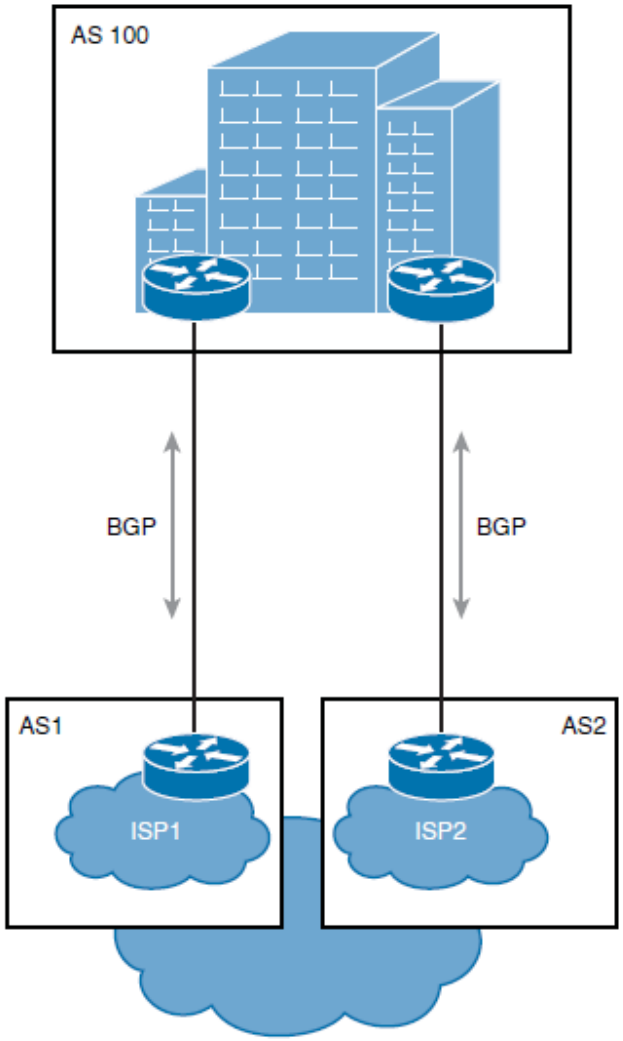



```
!GW1 has default route to one ISP router
ip route 0.0.0.0 0.0.0.0 209.165.201.129
router eigrp 1
 redistribute static metric 20000 1 255 1 1500

!GW2 has default route to the other ISP router
ip route 0.0.0.0 0.0.0.0 209.165.202.129
router eigrp 1
 redistribute static metric 10000 1 255 1 1500
```

Multihomed Internet Connectivity

- The multihomed Internet design offers the highest level of redundancy. It resolves all single points of failure issues and provides a reliable link to the Internet.
- Two routers are commonly used as Internet gateways, and each router is connected to a different ISP using one or more physical links.

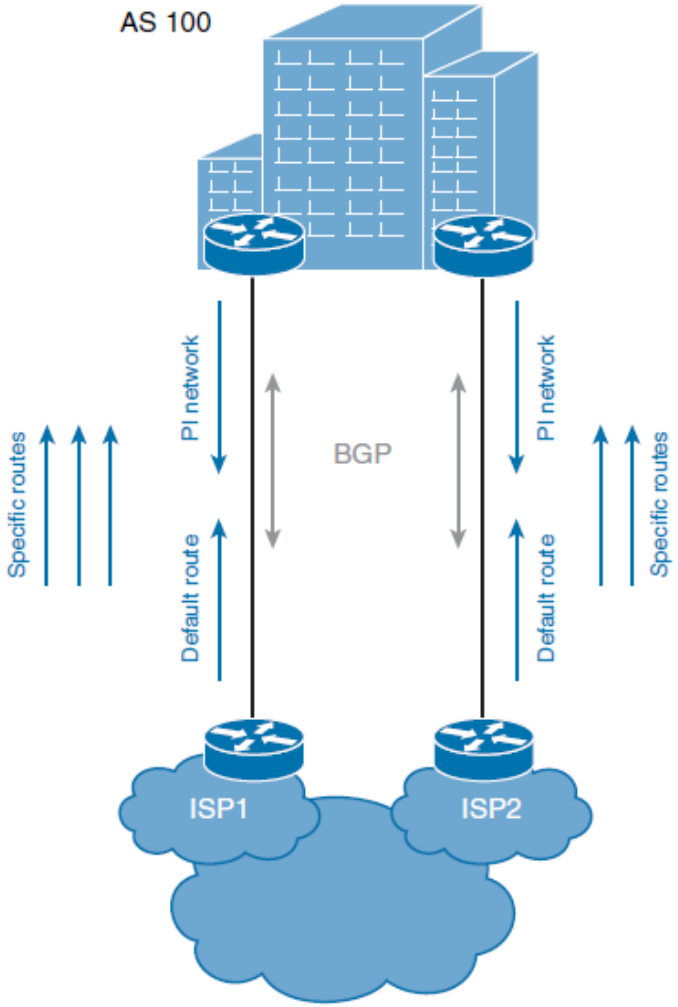


Multihomed Internet Connectivity

- Establishing a multihomed environment involves meeting some requirements:
  - You must have PI (Provider Independent) address space and your own autonomous system number.
  - You must establish connectivity with two independent ISPs.

Options for Routes That ISPs in a Multihomed Design Can Send

- The ISPs can send the following to your network:
  - The ISPs can send only a default route.
  - The ISPs can send a partial routing table and a default route.
  - The ISPs could also send you a full routing table.



Chapter 6 Summary

- Internet connectivity requirements: outbound only, or also inbound.
- Internet connectivity redundancy options: edge device, link, and ISP.
- The four connection redundancy types:
  - **Single-homed:** One connection to one ISP
  - **Dual-homed:** Two connections to one ISP
  - **Multihomed:** One connection to each of multiple (usually two) ISPs
  - **Dual multihomed:** Two connections to each of two ISPs
- Public IP address assignment: The IANA assigns to RIRs; RIRs assign to ISPs and organizations.

Chapter 6 Summary

- IP addresses, which can be PI or PA.
- Routing protocols that are either IGPs (and operate within an autonomous system) or EGPs (and operate between autonomous systems). BGP is the protocol used between autonomous systems on the Internet.
- The range of private autonomous system numbers: 64,512 to 65,534 and 4,200,000,000 through 4,294,967,294 (64,086.59904 through 65,535.65534).
- Provider-assigned IPv4 addresses, which can be configured statically or via DHCP.
- DHCPv4 operation, including the DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and DHCPACK messages.
- The use of NAT for IPv4, typically to translate private addresses to public addresses.

Chapter 6 Summary

- The four types of NAT addresses:
  - **Inside local address:** The IPv4 address assigned to a device on the internal network.
  - **Inside global address:** The IPv4 address of an internal device as it appears to the external network. This is the address to which the inside local address is translated.
  - **Outside local address:** The IPv4 address of an external device as it appears to the internal network. If outside addresses are being translated, this is the address to which the outside global address is translated.
  - **Outside global address:** The IPv4 address assigned to a device on the external network.
- The three types of NAT: static (one-to-one), dynamic (many-to-many), and PAT (many-to-one).
- The order of operations for NAT: It first performs routing and then translation when going from an inside interface to an outside interface, and vice versa when the traffic flow is reversed.

Chapter 6 Summary

- NAT issues, including when an inside device tries to communicate with a device on another inside interface.
- NVI, which removes the requirement to configure an interface as inside or outside. NVI also operates differently; it performs routing, translation, and routing again. The whole process is symmetrical, no matter which way the traffic is flowing.
- Configuring a Cisco router to be a DHCP server and a DHCP relay agent, for both IPv4 and IPv6.
- IPv6 addresses, which can be configured with the following methods:
  - Manual Assignment
  - SLAAC
  - Stateless DHCPv6
  - Stateful DHCPv6
  - DHCPv6-PD

Chapter 6 Summary

- DHCPv6 operation, including the SOLICIT, ADVERTISE, REQUEST, and REPLY messages.
- Two types of NAT for IPv6: NAT64 and NPTv6.
- IPv6 ACLs, which include three implicit rules at the end of each ACL, as follows:
  - **permit icmp any any nd-na**
  - **permit icmp any any nd-ns**
  - **deny ipv6 any any**
- Applying an IPv6 ACL to an interface, using the **ipv6 traffic-filter** *ACL-name* { **in|out** } interface configuration command. Notice the **traffic-filter** keyword is used rather than the **access-group** keyword that is used in IPv4 ACLs.
- The need to secure devices connected to the IPv6 Internet.
- The drawbacks of single-homed Internet connectivity because of the single points of failure: link failure, ISP failure, or router failure.

Chapter 6 Summary

- Using a dual-homed design to improve redundancy: two (or more) connections, using one or more Internet routers, to the same ISP. The ISP may also have multiple routers to connect to specific customers. Static routes or BGP are used. One link can be primary, or traffic can be load balanced over both links.
- Using a multihomed design to further improve redundancy; two routers are used as Internet gateways, and each router is connected to a different ISP using one or more physical links.
- The options for what ISPs can send to your network in a multihomed design:
  - Only a default route
  - A partial routing table (of a subset of routes originated near the ISP) and a default route
  - A full routing table
- How receiving full routing tables consume a lot of router resources.