



Modul/stretnutie 1



ROUTE Module 1

Pavel Segeč

Program stretnutia

- Dokumentácia na webe Cisco
- Pohľad na dizajn sietí
- Základy smerovania v IPv4 sieťach
 - Základné fakty o adresovaní a smerovaní
 - Špecifiká NBMA sietí
 - Pár faktov o smerovacích protokoloch
- Konfigurácia:
 - Použitie /31 masiek na point-to-point linkách
 - IP Unnumbered
 - Statické smerovacie položky
 - On Demand Routing (ODR)
 - RIPv2
- Frame relay?

Dokumentácia na webe Cisco




Dokumentácia na webe Cisco

- Kurikulá ani tieto kurzy nemajú ani ambíciu, ani šancu obsiahnuť dopodrobna všetky príkazy a ich úplnú syntax
 - Detaily, vysvetlenie nejasností a doplňujúce informácie je potrebné hľadať na web stránkach Cisca
- Orientácia na webe Cisca je pre budúcich sieťových profesionálov vecou prežitia
 - Cisco má veľmi rozsiahlu informačnú bazu
 - Štruktúra nie je na prvý pohľad intuitívna
 - Pre nás je obzvlášť zaujímavá **produktová dokumentácia** a podporné dokumenty

Dokumentácia na webe Cisco

- Produktová dokumentácia je k dispozícii
 - Pre jednotlivé hardvérové platformy
 - Pre jednotlivé verzie operačných systémov
- Praktické skúsenosti ukázali, že
 - Príkazy IOSu **na smerovačoch** je vhodné hľadať rovno v dokumentácii **k príslušnému IOSu**
 - Príkazy IOSu **na prepínačoch** je vhodné hľadať v produktovej dokumentácii **prepínača**
 - Príkazy IOSu na prepínačoch často nie sú v manuáloch k „veľkému“ IOSu dokumentované, zrejme kvôli samostatnej vetve vývoja IOSu pre prepínače
- Pred hľadaním dokumentácie je vhodné zistiť si aktuálnu verziu IOSu, ku ktorému hľadáme popis
 - sh version


http://cisco.com/go/support

[Products & Services](#)[Support](#)[How to Buy](#)[Training & Events](#)[Partners](#)

[Worldwide](#)[Log In](#)[Account](#)[Register](#)

Product Support

Troubleshooting, configuration, installation, and technical documentation



 [Support Community Forums](#)



Product Categories

[Routers](#)[Switches](#)

[Security](#)[Wireless](#)[Cisco IOS and NX-OS Software](#)

[Voice and Unified Communications](#)

 [Linksys Home](#) [Valet](#)

 [Flip Video](#) [ūmi telepresence](#)

[Small Business Support](#)[All Products](#)

Downloads

VPN Client drivers, firmware, NOS, and application software


Popular Downloads


- [VPN Client v5.x](#)
- [Cisco RV042 Dual WAN VPN Router](#)
- [ASA 5500 Series](#)
- [Cisco Configuration Professional](#)
- [Cisco Network Assistant Version 5.0](#)
- [Cisco IP Communicator](#)
- [Cisco Configuration Assistant \(CCA\)](#)
- [Cisco WRVS4400N Wireless-N Gigabit Security Router - VPN V2.0](#)


[All Downloads](#)

Contacts/Support Cases

Open/View a TAC Support Case



[My Support Cases](#) 

[Ordering and Contract Management](#) 


[RMA Return Instructions](#)


[Warranty Information](#)

Small Business

[Support Center Contacts](#)

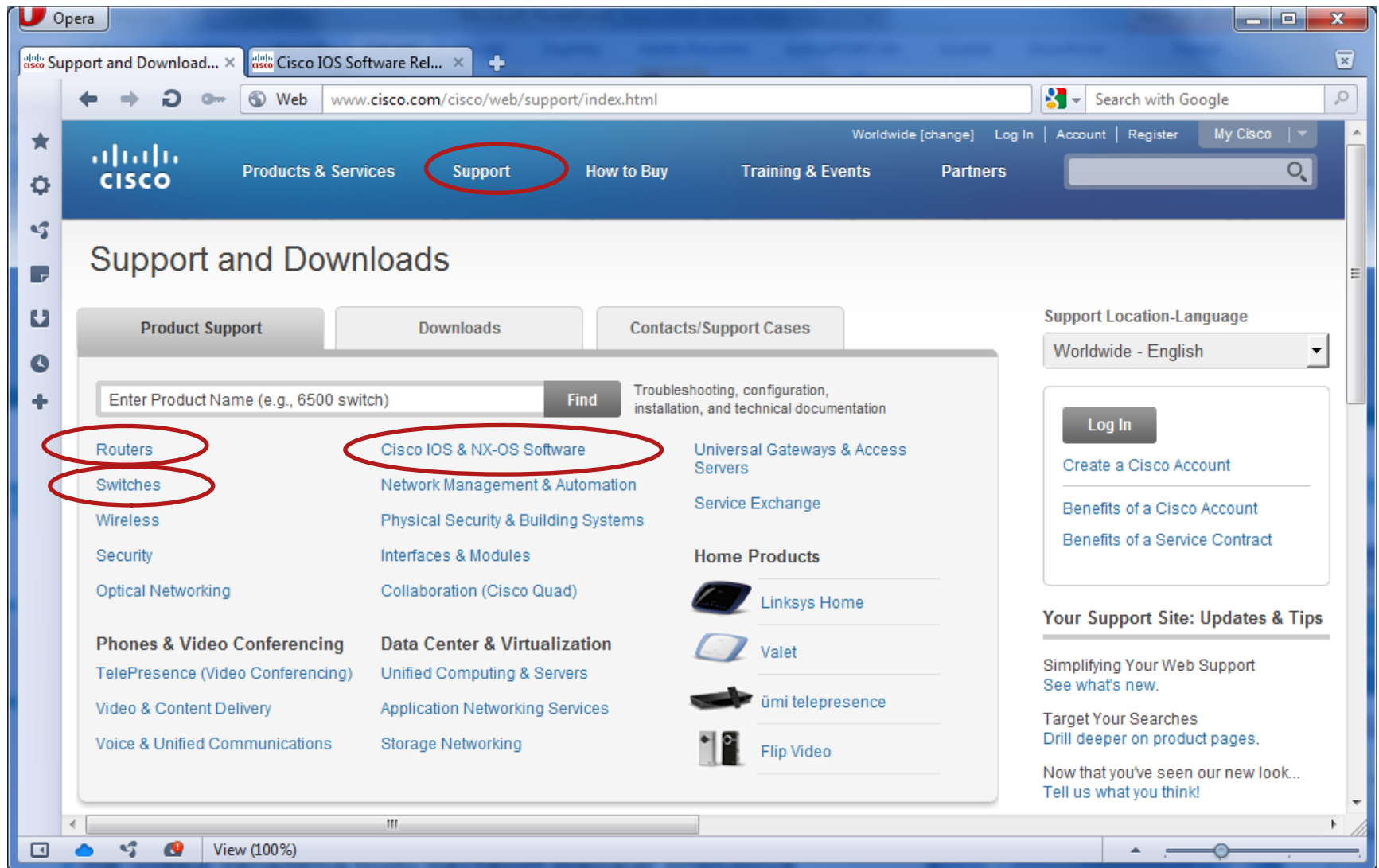
[Community](#)

 [Call or Email Technical Support](#)

 Additional Entitlement Required

[All Support](#)

http://cisco.com/go/support



Dokumentácia k IOS

- V dokumentoch k IOSu sú pre nás najdôležitejšie tieto časti:
 - **Configuration Guides**: obsahujú popis jednotlivých technológií či protokolov a spôsob ich konfigurácie
 - **Command References**: obsahujú popis jednotlivých príkazov, ich syntax a účinok
 - **Master Index**: obsahuje abecedne usporiadaný zoznam príkazov s odkazmi na Command Reference
 - **Error and System Messages**: obsahuje zoznam jednotlivých hlásení IOS a ich vysvetlenie
- Alternatívne je možné použiť Command Lookup Tool pre vyhľadanie Command Reference k danému príkazu
 - Je však potrebné mať CCO account (stačí aj guest level)
 - Je potrebné sa pred prvým použitím prihlásiť
 - <http://tools.cisco.com/Support/CLILookup/cltSearchAction.do>

Podporná dokumentácia

- Rôzne ďalšie dokumenty obsahujú prípadové štúdie, rozbery princípov, technológií, príklady konfigurácií
- Mnohé z nich sú identifikované číslom *Document ID*
- Ako ich vyhľadávať?
 - „Configuring ...“
 - „Understanding ...“
 - „Troubleshooting ...“
 - „How to ...“
 - Support → Cisco IOS and NX-OS Software → Technology
- Dokumenty sa mnohokrát odkazujú na ďalšie
 - **Je vhodné robiť si záložky!**

Dizajn sietí

Modely a nástroje



Trojvrstvový model siete

- S postupným rastom siete sa v nej nachádza čoraz viac zariadení
- Je preto výhodné rozdeliť ich podľa funkcie, ktorú majú v sieti plniť, a organizovať ich vo vrstvách:
 - Isté zariadenia budú slúžiť na pripájanie koncových zariadení k sieti
 - Iné, vyššie zariadenia budú navzájom prepájať prístupové zariadenia. Pritom môžu vykonávať bezpečnostné alebo ukončovacie (terminujúce) operácie
 - Zariadenia na najvyššej úrovni budú tvoriť chrbticu celej siete
- Hierarchický systém troch vrstiev – prístupovej, distribučnej a chrbticovej je starší model siete

Vlastnosti dobre navrhutej siete

- Kľúčom k dobrému návrhu siete je jej hierarchický dizajn
- Hierarchická sieť:
 - Ohraničuje veľkosť a rozsah kolíznych, broadcastových a chybových domén
 - Zjednodušuje činnosť rôznych mechanizmov, ktoré pracujú v jednotlivých oblastiach sietí
 - Dovoľuje efektívne pridelovať adresy a ľahko ich sumarizovať v smerovacích protokoloch
 - Sprehľadňuje toky dát
 - Jasne oddeľuje funkčné bloky pre L2 a L3
- Dobrý model siete podporuje jej:
 - Škálovateľnosť, Redundanciu,
 - Výkonnosť, Bezpečnosť,
 - Manažovateľnosť Udržovateľnosť.

Funkcie vrstiev trojvrstvového modelu

■ Prístupová vrstva

- Obvykle prepínaná, v poslednej dobe i smerovaná
- Prístup klientov do siete, zadelenie do VLAN, bezpečnostné mechanizmy pri prístupe a komunikácii, QoS mechanizmy
- Vo WAN prostredí zabezpečuje prístup z pobočiek a teleworkerom prístup do podnikovej siete

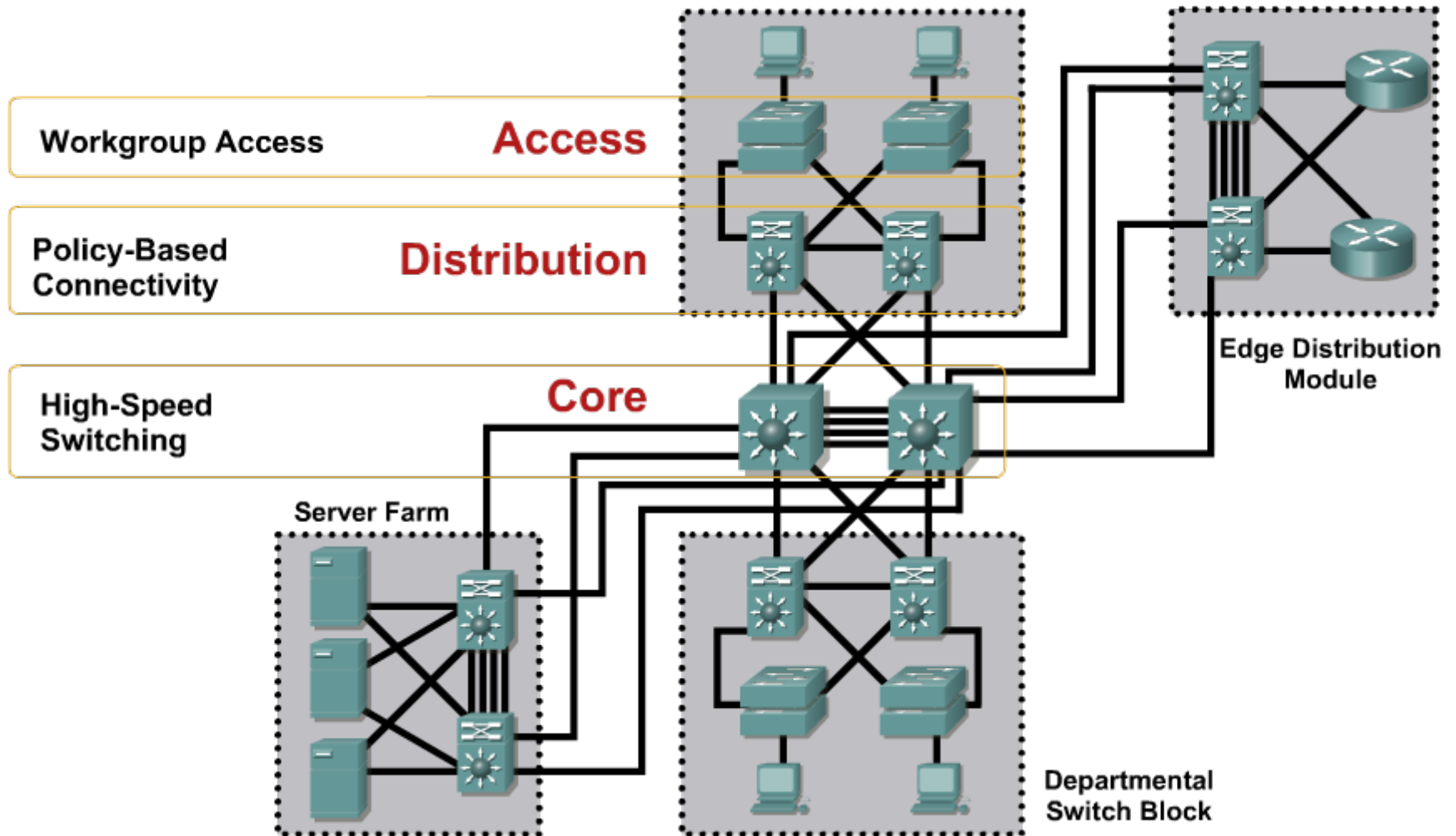
■ Distribučná vrstva

- Obvykle smerovaná
- Ukončenie VLAN, smerovanie medzi nimi, sumarizácia adresových rozsahov z prístupovej vrstvy, bezpečnostné mechanizmy pri komunikácii, QoS mechanizmy, oddelenie chybových domén

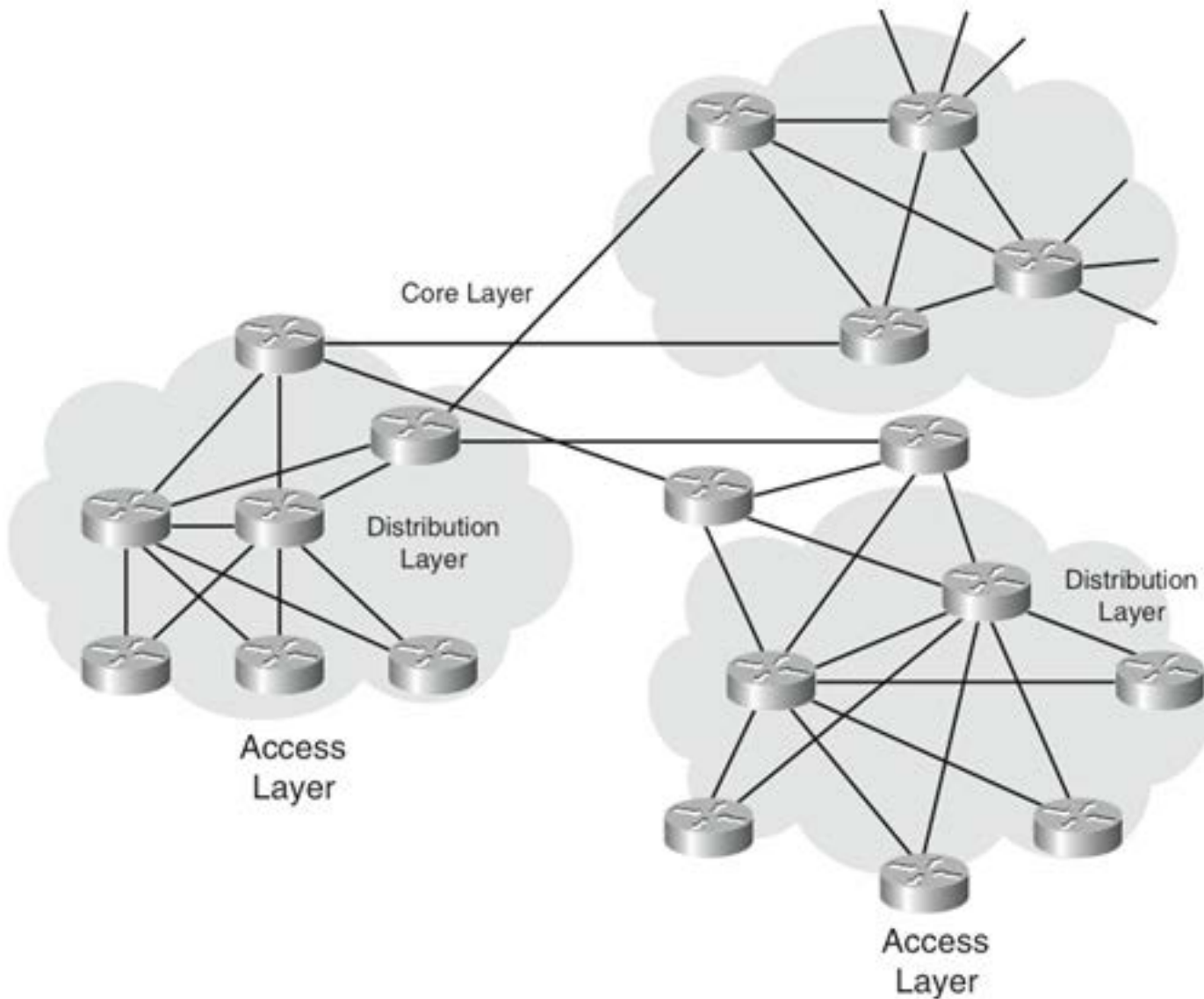
■ Vrstva jadra (chrátnica)

- Obvykle smerovaná s nutnosťou rýchlej konverencie
- Redundantné prepojenia s dostatočnou kapacitou, vysokorýchlostné prepínanie a smerovanie, QoS mechanizmy

Tradičný trojvrstvový model príklad prepínanej campus siete



Tradičný trojvrstvový model príklad WAN siete



Komplexné konvergované siete

- Konvergovaná sieť je mix typov aplikácii, služieb a prevádzok:
 - **Voice and video traffic**
 - IP telefónia, video, konferencie
 - Jedná sa o real-time dáta a tie vyžadujú použitie QoS nástrojov pre garanciu ich včasného doručenia
 - **Voice applications traffic**
 - Dáta súvisiace s prevádzkou hlasových služieb, napr. kontaktné centrá
 - **Mission-critical traffic**
 - Aplikácie kľúčového významu pre podnik
 - **Transactional traffic**
 - Aplikácie pre e-commerce
 - **Routing protocol traffic**
 - Prevádzka generovaná smerovacími protokolmi
 - **Network management traffic**
 - Dohľadové protokoly nad sieťou
- Sieťové požiadavky sú rozličné podľa mixu prevádzky, najmä v oblasti výkonnosti a bezpečnosti
- Potreba nových modelov

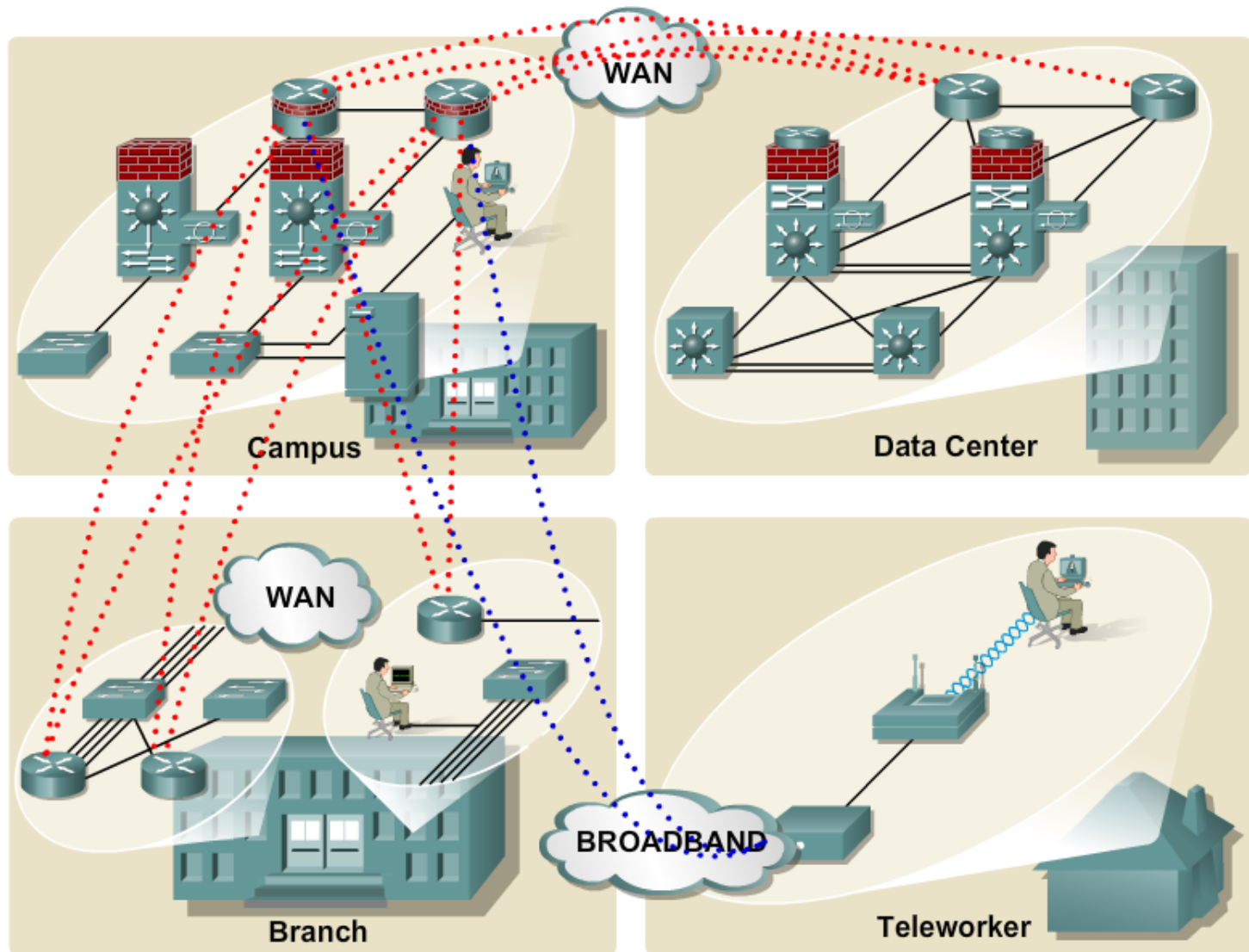
Návrh veľkých (komplexných) sietí

- Návrh rozľahlejších sietí je netriviálna záležitosť, ktorá si vynucuje komplexnejší model
 - než klasický 3-vrstvový hierarchický model
 - Jednoduchý a úspešný
 - Nie je veľmi detailný, nezohľadňuje vlastné potreby siete
- Existuje množstvo metodík, ako siete navrhovať
 - Z pohľadu architektúry (topológie)
 - Z pohľadu platných nariadení, resp. predpisov
 - Z pohľadu poskytovaných služieb
 - Z pohľadu inteligencie a prepojenia s inými systémami

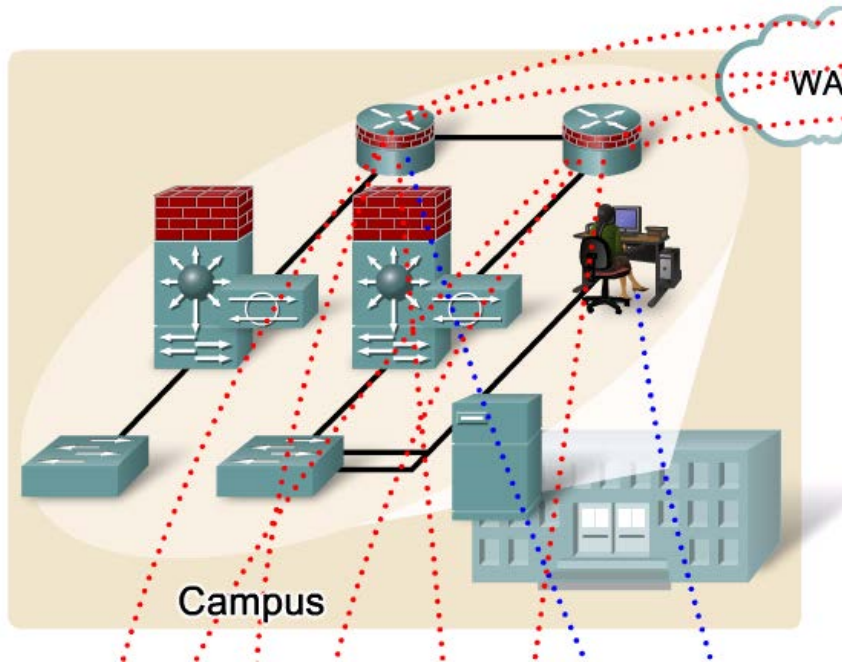
Návrh veľkých sietí

- Model pre rozľahlé podnikové siete - „Cisco Enterprise Architecture“
 - Zohľadňuje logické bloky bližšie popisujúce organizáciu siete podniku
 - Definuje časti siete (moduly) a ich **jasné hranice** podľa ich funkcie
 - 6 základných častí:
 - Enterprise Campus, Enterprise Edge, Provider (Edge), Enterprise Branch, Enterprise Data Center, Enterprise Teleworkers
 - Každá z týchto častí má odporúčanú architektúru a riešenia
 - Je plne škálovateľný
 - Rozširuje hierarchický model
 - Uľahčuje rast a rozširovanie siete pridávaním ďalších modulov
 - Bloky/moduly je možné podľa potreby pridávať

Cisco Enterprise Architecture



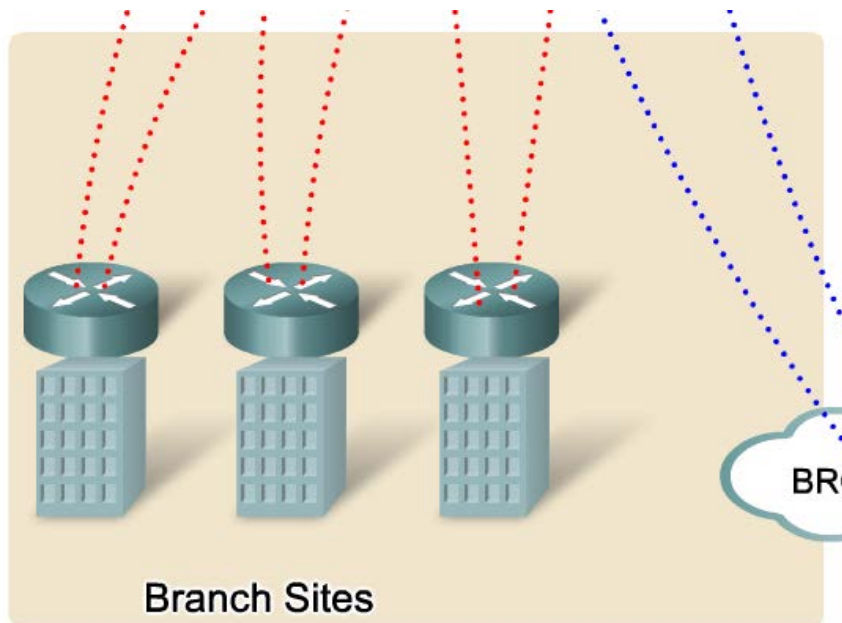
Cisco Enterprise Campus Architecture



■ Poskytuje :

- Vysokú dostupnosť (HA) s prvkami multilayer prepínania a redundanciou HW a SW
- Automatické procedúry pre rekonfiguráciu siete a sieť. ciest pri výskyte chýb
- Multicast služby pre optimalizované doručovanie dát
- Quality of Service (QoS)
- Integrovanú bezpečnosť
 - IEEE and EAP
- Flexibilitu pridať IP security (IPsec), MPLS VPNs, riadenie identít a prístupu, VLANs

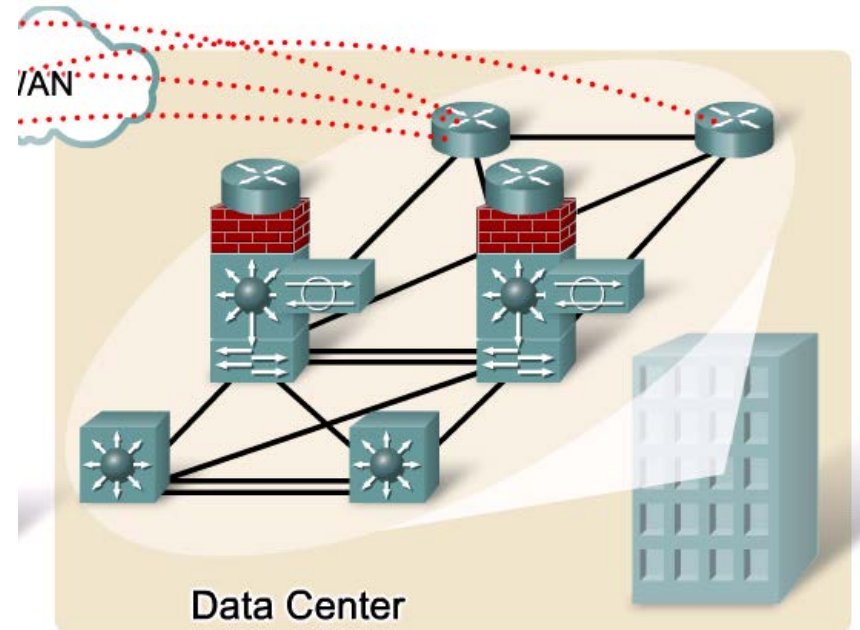
Cisco Enterprise Branch Architecture



- Umožňuje a rozširuje využívanie služieb centrál pobočkám
 - Bezpečnosť, Cisco IP communications (unified comm. – voice/video), iné aplikácie centrál (mission critical)
- Cisco využíva Integrated service routers (ISR) umiestnené na pobočkách
 - ISR integruje prvky ako bezpečnosť, pokročilé smerovanie, sieťové analýzy, caching, konvergencia hlasu a videa, VPN, WAN redundanciu
- Podnik stále môže centrálné riadiť, monitorovať a manažovať zariadenia pobočiek.

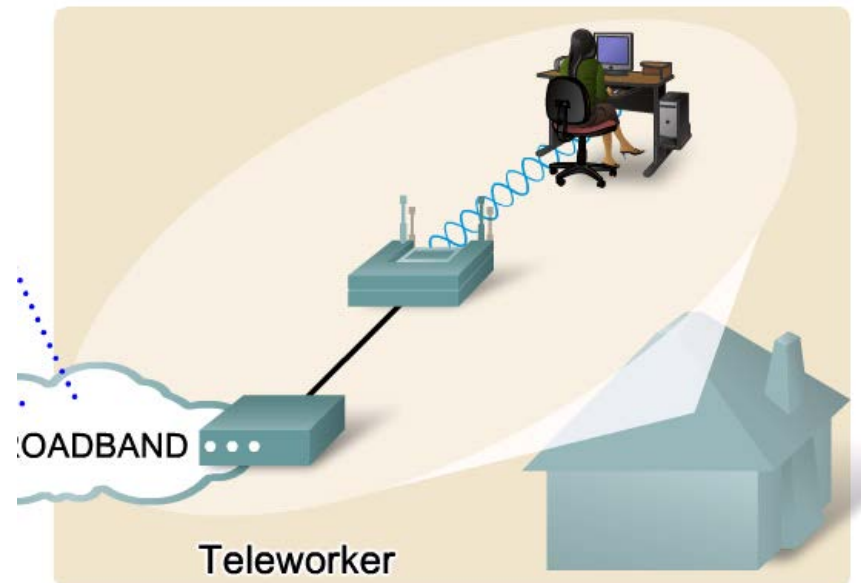
Cisco Enterprise Data Center Architecture

- Adaptabilná sieťová architektúra, ktorá podporuje požiadavky na konsolidáciu, zabezpečenie kontinuity podnikových procesov, bezpečnosť.
 - A umožňuje servisne orientovanú arch., virtualizáciu, on-demand computing
- Staff a zákazníci majú poskytnutý
 - Bezpečný prístup k aplikáciám a zdrojom, zjednodušuje manažment a redukuje režijné a mimoriadne výdaje
- Dátové centra poskytujú
 - Redundáciu
 - Zálohovacie riešenia
 - Pre synchr/asynchr. replikáciu dát a aplikácii
 - Zariadenia ponúkajú aplikačný load balancing
 - Umožňuje škálovateľnosť infraštruktúry bez prerušení



Cisco Enterprise Teleworker Architecture

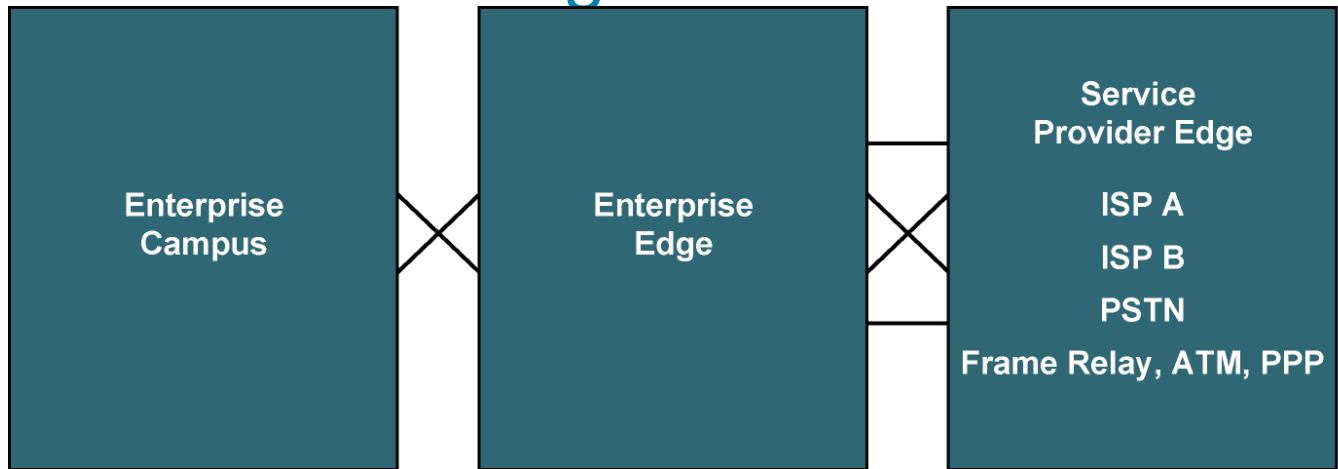
- Nazývané aj ako *Enterprise Branch-of-One*
- Umožňuje bezpečné doručovanie hlasových a dátových služieb centrály malým SOHO používateľom
 - Cez štandardné internetové širokopásmové pripojenie
- Využíva centralizovaný manažment
 - Zníženie nákladov
- Bezpečnostná politika využíva robustné integrované bezpečnostné riešenia a na identite založené sieťové služby
 - always-on VPN



Best practises

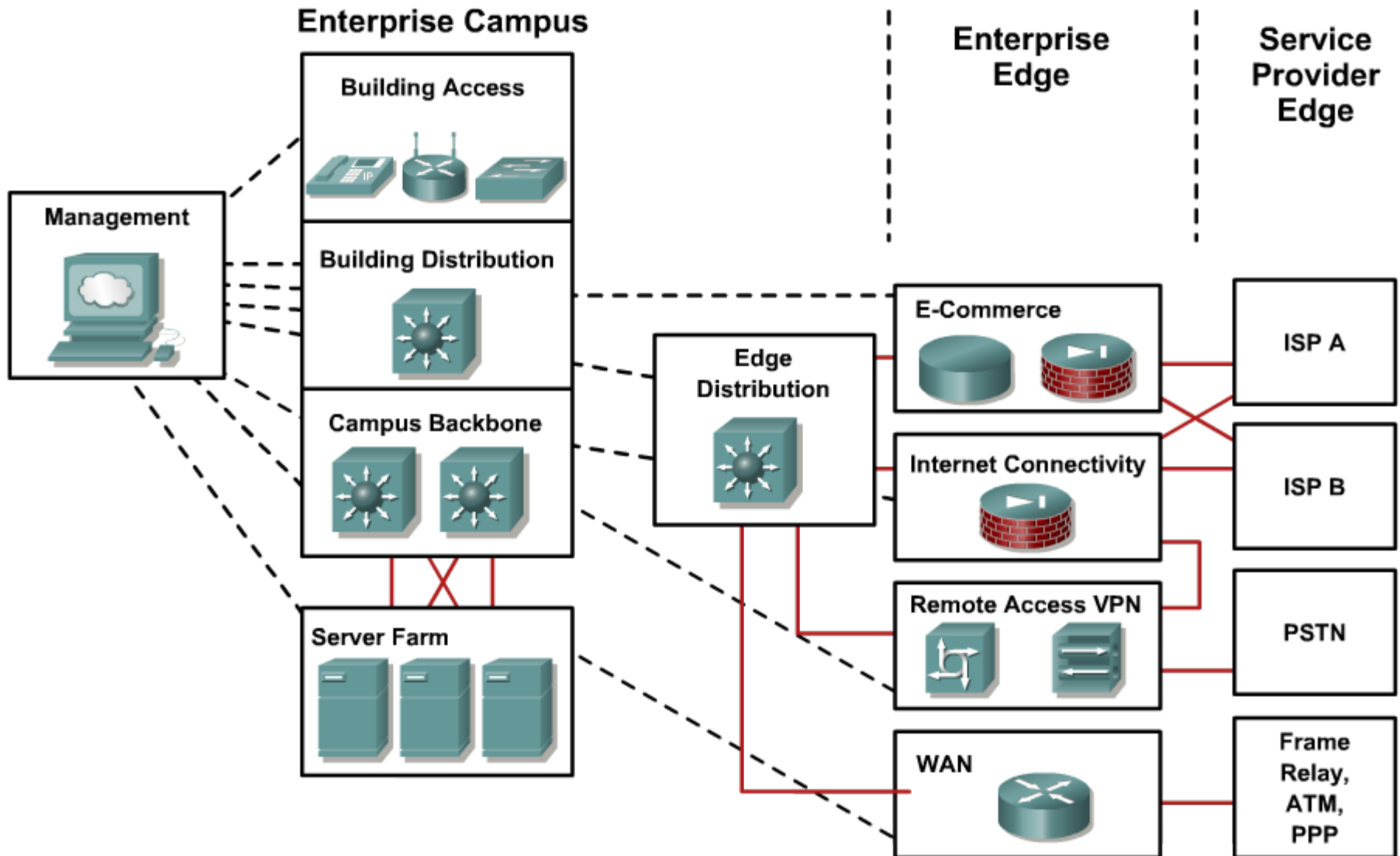
- Enterprise Composite Network Model

<http://www.cisco.com/go/safe>

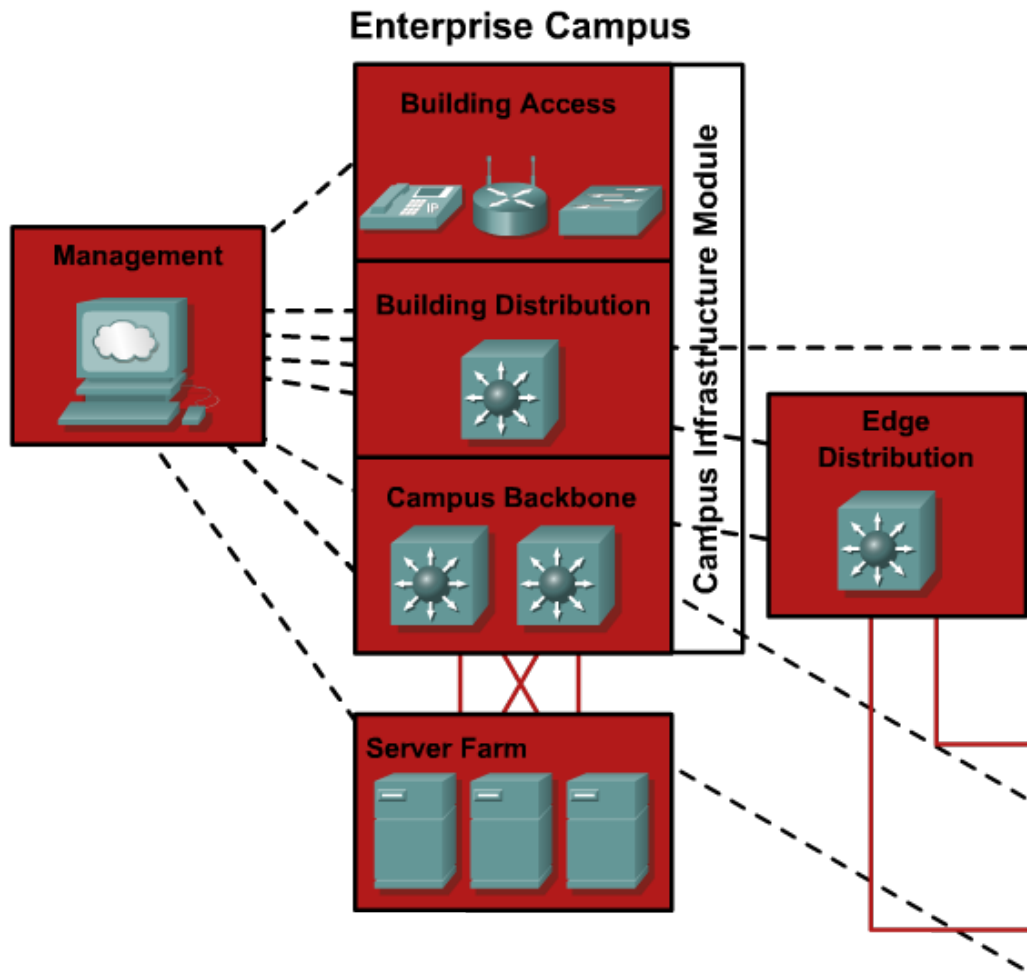


- Je dizajnový a implementačný framework pre [Cisco Enterprise Architecture](#)
- Tri základné funkčné oblasti
 - **Enterprise Campus**
 - Obsahuje moduly na vybudovanie výkonnej a robustnej campus firemnej siete
 - **Enterprise Edge**
 - Množina funkcií týkajúcich sa externého prístupu do firemnej siete
 - Pobočky, internet, vzdialený používatelia
 - **Service Provider Edge**
 - Prístup k sieťovým zdrojom mimo firemnej siete
 - ISP, WAN poskytovatelia, PSTN

Enterprise Composite Network Model

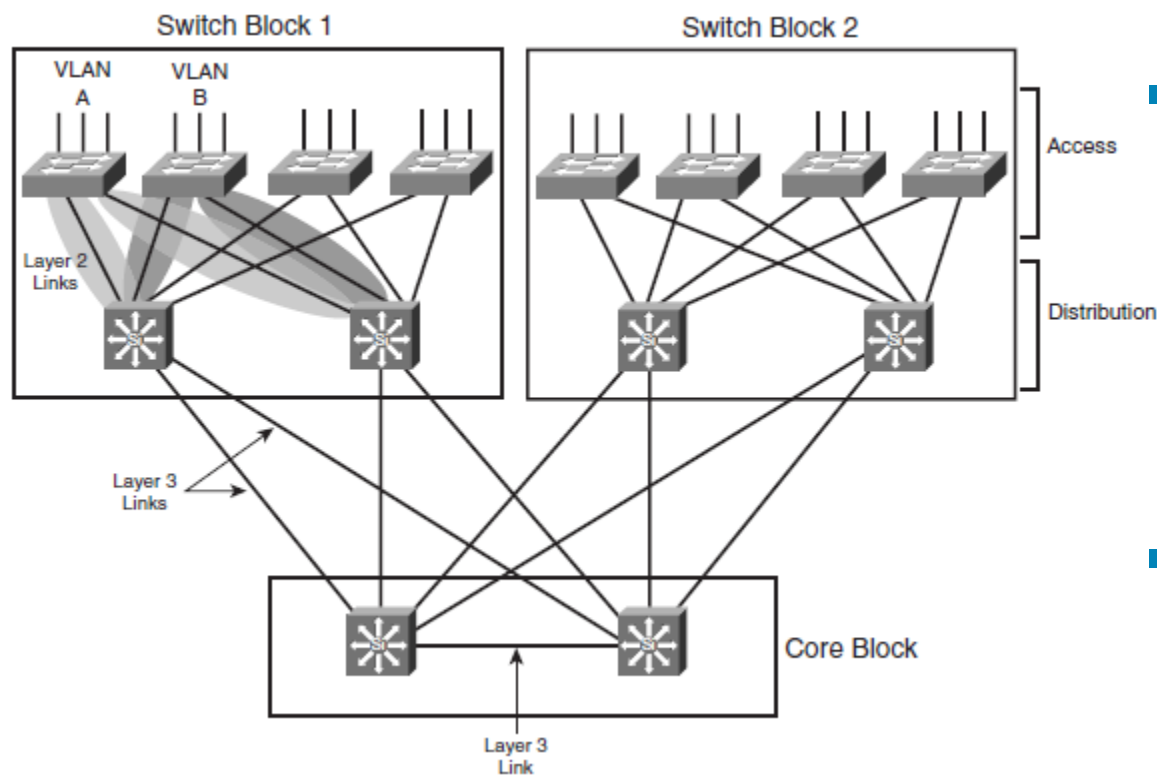


Moduly v bloku Enterprise Campus



- **Campus Infrastructure module**
 - **Switch block**
 - Building Access
 - Building Distribution
 - **Core block**
 - Campus backbone
- **Server farm block**
 - Servery ponúkajúce služby pre celý campus
 - Sú vysokorychlostne duálne pripojené na sieť
- **Management block**
 - Network monitoring, System logging, Authentication, authorization, and accounting (AAA), Policy-management applications, System administration and remote-control services, Intrusion-detection management applications
- **Edge Distribution block**
 - Agreguje konektivitu

Modul Campus Infrastructure



- V duchu hierarchického dizajnu
- Switch block (or building switch block)
 - Zahŕňa **access** a **distro** prepínače (block) per každú budovu campusu
 - Preto “*Building*”
- Core block
 - Dual core (obr.)
 - Collapsed



IIN & SONA



Cisco IIN stratégia a SONA framework

- Pre Cisco je sieť viac než len súvislá komunikačná infraštruktúra – je to platforma pre integrované aplikácie
 - Sieť sa však musí stať „application-aware“
- *Intelligent Information Network* (IIN) je evolučná vízia novej siete, v ktorej prvky aktívne spolupracujú
 - Integrácia sieťových informačných zdrojov
 - Integrácia IT infraštr. so sieťou
 - Inteligencia sieťových prvkov a platforiem
 - Aktívna participácia siete na poskytovaní aplikácii a služieb
 - Umožňuje sieti sa aktívne podieľať na riadení, monitorovaní a doručovaní služieb
- IIN je stratégia, ktorá rieši ako je sieť integrovaná s podnikom a podnikovými prioritami
 - Poskytuje centralizované a unifikované riadenie s end-to-end funkcionalitami

Fázy Cisco Intelligent Information Network

- IIN architektúra podľa Cisco vzniká v troch etapách (fázach):

1. Integrovaný transport

- Everything over IP
- Spoločná konsolidovaná (konvergovaná) IP sieť pre všetky druhy sieťových tokov a služieb

2. Integrované služby

- Združovanie (pooling), zdieľanie a virtualizácia IT zdrojov za účelom pružného reagovania na potreby organizácie
- Unifikácia kapacity sieťových úložísk a dátových centier
- Virtualizácia serverov, úložísk a sieťových prvkov

3. Integrované aplikácie (Application-Oriented Networking, AON)

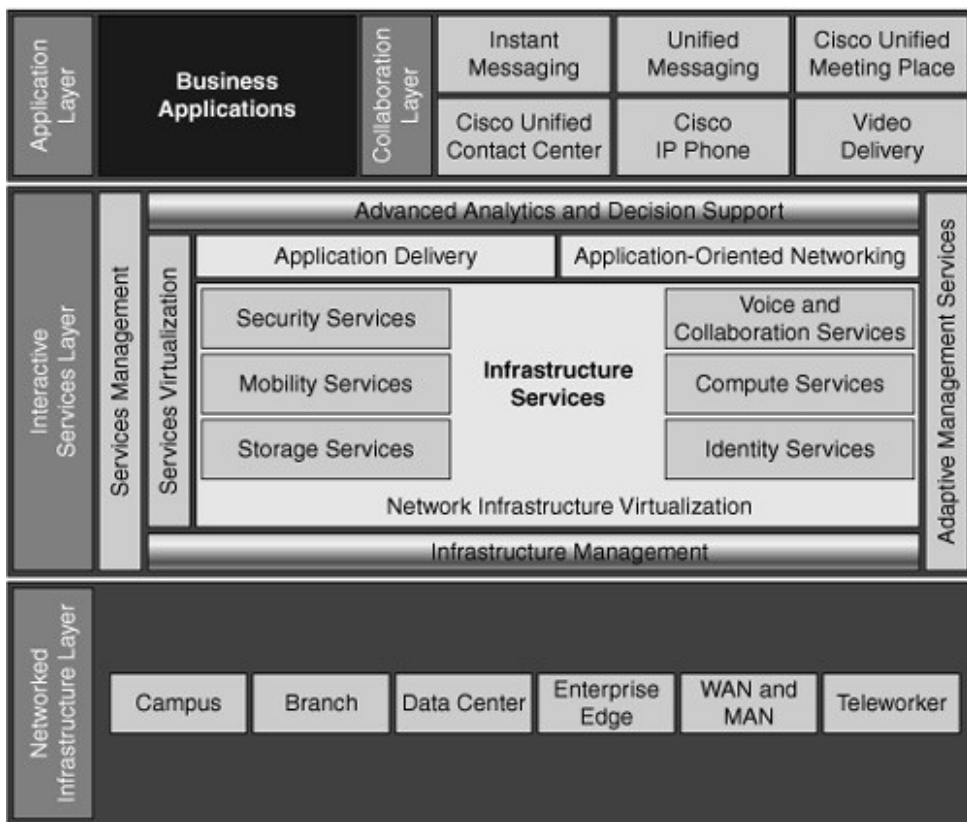
- Inteligentná sieť rozoznávajúca, aký druh služby poskytuje a podľa toho optimalizuje svoju činnosť (application-aware network)
- Content caching, application load balancing, aplikačná bezpečnosť
- 2. fáza IIN je v súčasnosti úplne bežná, 3. fáza pomaly prichádza

Service Oriented Network Architecture

<http://www.cisco.com/go/sona>

- *Service Oriented Network Architecture* (SONA) je architekturný framework pre IIN
 - Sieťová infraštruktúra z podstatne vyššieho pohľadu
 - Poskytuje návody a odporúčania ako prepájať sieťové služby a aplikácie do integrovaných biznis riešení
 - Smer IIN
 - Dá sa povedať, že ECNM + SONA = IIN
- SONA organizáciám umožňuje
 - Zvýšenie flexibility, efektívnosti optimalizáciou aplikácií, biznis procesov, zdrojov.
- SONA framework má tri vrstvy
 - Networked Infrastructure Layer
 - Interactive Services Layer
 - Application Layer

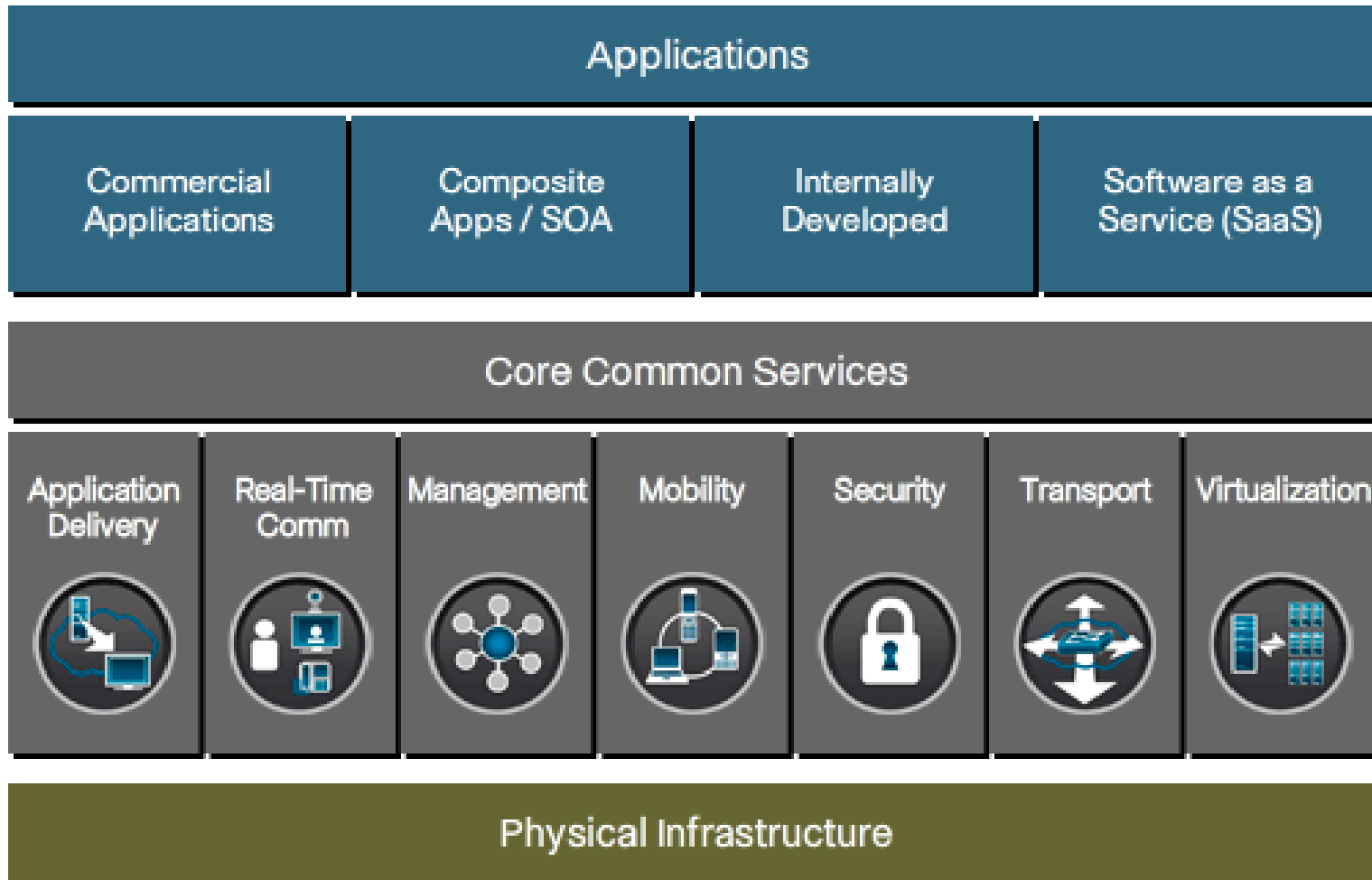
Vrstvy Cisco SONA Framework



- Networked Infrastructure Layer
 - Všetky IT zdroje (servery, klienti, storage) prepojené cez konvergovanú infraštruktúru (LAN/MAN/WAN)
 - ECNM
- Interactive Services Layer
 - Podporuje alokáciu zdrojov aplikáciám a biznis procesom cez sieť
 - Zahŕňa
 - hlas a kolaboračné služby, mobilita, bezpečnosť a identifikačné služby, storage, výpočtové služby, virtualizácia sieť. infraštruktúry, manažment služieb
- Application Layer
 - Samotné biznis a spolupracujúce aplikácie

SONA update

<http://www.cisco.com/go/sona>



Cisco Borderless Networks

<http://www.cisco.com/go/borderless>

- Nový dizajnový rámec
- Biznis naprieč hraniciam siete
 - Prístup k zdrojom kdekoľvek a kedykoľvek
 - Zvyšovanie produktivity
 - Znižovanie biznis a IT nákladov
- Clouds



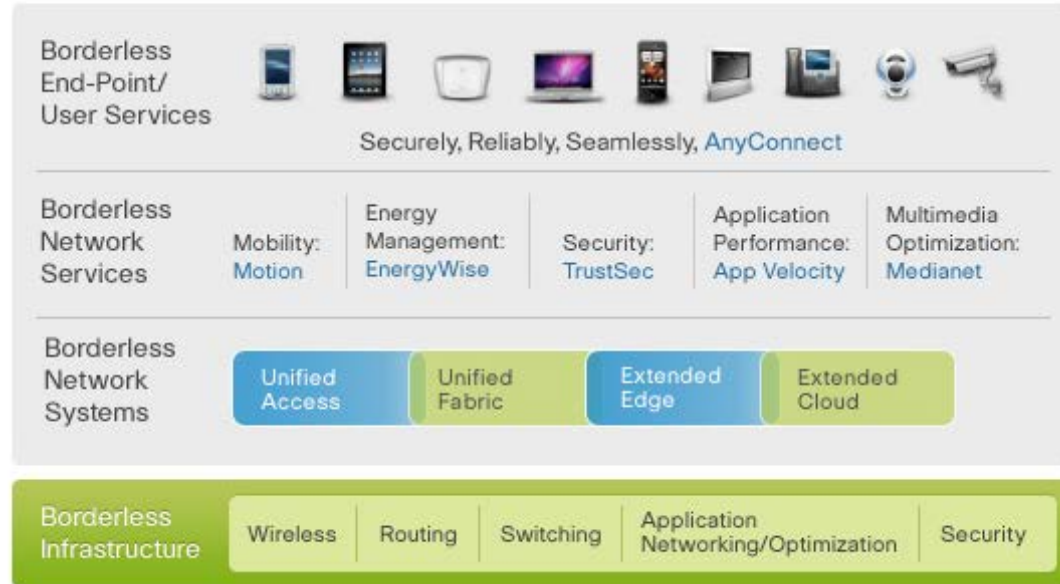
Policy

Management

APIs



Borderless Network Architecture Architecture for Agile Delivery of the Borderless Experience





Metodiky návrhu a implementácie sietí



Metodiky návrhu a prevádzky siete

- Pre návrh a prevádzku siete existuje viacero metodík
 - FCAPS – Fault, Config, Accounting, Performance, Security (ISO)
 - TMN – Telecommunication Management Network (ITU-T)
 - ITIL – IT Information Library
 - Cisco Lifecycle Services (PPDIOO)
- Cisco Lifecycle Services sa niekedy označuje aj ako model PPDIOO podľa názvov šiestich fáz, z ktorých sa skladá
 - Prepare
 - Plan
 - Design
 - Implement
 - Operate
 - Optimize

Fázy návrhu PPDIOO (1) - Príprava

■ Prepare

- Stanovenie vízie a požiadaviek organizácie či podniku, návrh stratégie na ich dosiahnutie, určenie kľúčových technológií pre dané požiadavky, návrh high-level architektúry.
- Táto fáza by mala predstaviť „business case“

■ Plan

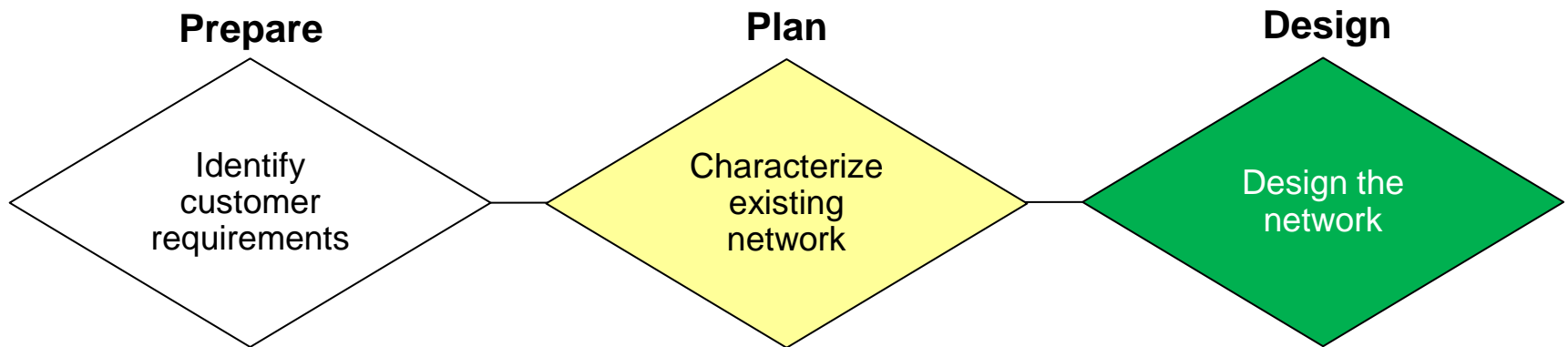
- Analýza a charakteristika danej siete. Určenie požiadaviek na sieťovú infraštruktúru, vyhodnotenie potrebných rozšírení a doplnení (tzv. gap analysis).
- Vypracovanie projektového plánu obsahujúceho jednotlivé úlohy, zodpovedných riešiteľov, časové etapy a potrebné zdroje na dizajn a implementáciu projektu.

■ Design

- Vytvorenie návrhu technickej infraštruktúry na základe informácií a požiadaviek z predchádzajúcich fáz.
- Projektový plán môže byť počas tejto fázy doplnený a spresnený.

Fázy návrhu PPDIOO (1) - Příprava

- The PPDIOO methodology begins with these three basic steps:
 - **Step 1: Identify customer requirements**
 - **Step 2: Characterize the existing network and sites**
 - **Step 3: Design the network topology and solutions**



- Once the design is defined, the implementation plan can be executed.

Fázy návrhu PPDIOO (2) - implementácia

■ Implement

- Implementácia riešenia vytvoreného vo fáze Design. Priebeh tejto fázy zahŕňa rozšírenie alebo prestavbu existujúcej sieťovej infraštruktúry.
- Každý zásah musí byť vopred ohlásený a autorizovaný, vždy by mal byť pripravený aj núdzový plán pre návrat do predošlého stavu. Bez vplyvu na výkonnosť a dostupnosť siete.

■ Operate

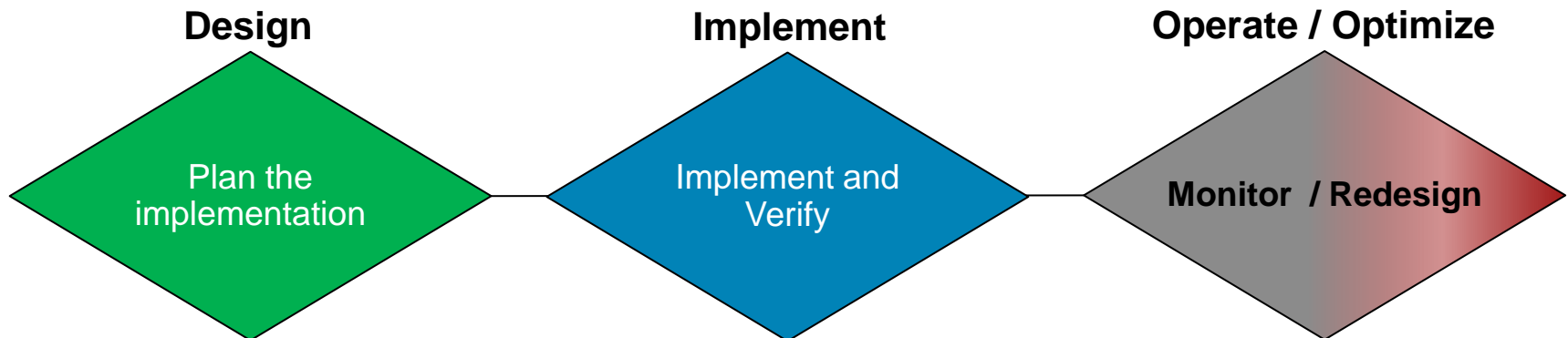
- Fáza, v ktorej sa implementované riešenie používa v rutínnej prevádzke.
- Súčasne sa získavajú prevádzkové informácie, realizuje sa rutinná údržba riešenia, aktualizácie, odstraňujú sa bežné chyby

■ Optimize

- Proaktívne sledovanie a manažment siete. Informácie o činnosti siete získané v tejto fáze môžu viesť k úprave riešenia a k ďalšej iterácii cyklu PPDIOO.

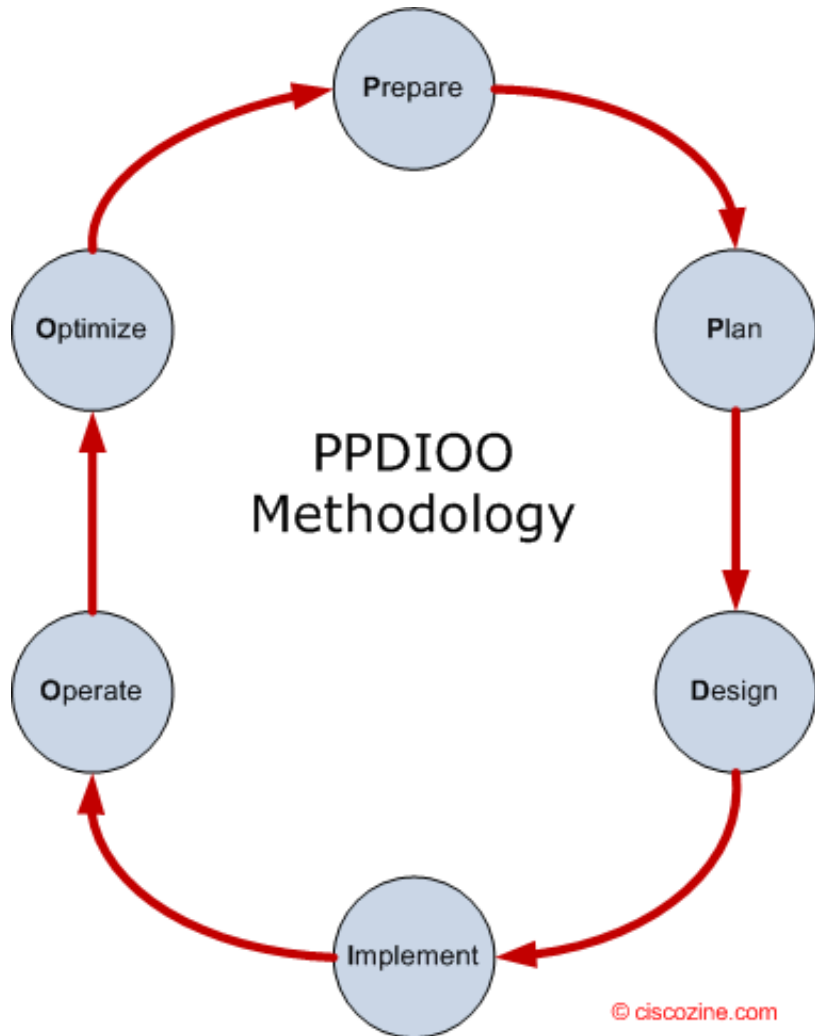
Fázy návrhu PPDIOO (2) - implementácia

- The next three steps include:
 - **Step 4: Plan the implementation:**
 - **Step 5: Implement and verify the design:**
 - **Step 6: Monitor and optionally redesign:**



Cisco Lifecycle Services

<http://www.cisco.com/warp/public/437/services/lifecycle/index.html>



■ Dôvody pre:

- Znižovanie celkových nákladov na vlastníctvo siete
- Zvyšovanie sieťovej dostupnosti
- Zlepšený prístup k aplikáciám a službám

Implementation Plan documentation

- The implementation plan documentation should include the following:
 - Network information
 - Tools required
 - Resources required
 - Implementation plan tasks
 - Verification tasks
 - Performance measurement and results
 - Screen shots and photos, as appropriate
- The documentation creation process is not finished until the end of the project, when the verification information is added to it.

Sample Implementation Plan

- Project contact list and statements of work, to define all of the people involved and their commitments to the project
- Site and equipment location information and details of how access to the premises is obtained
- Tools and resources required
- Assumptions made
- Tasks to be performed, including detailed descriptions
- Network staging plan

Project Contact List (sample)

Cisco Project Team	<Customer> Project Team
Project Manager: Telephone: Email:	Project Manager: Telephone: Email:
Project Engineer: Telephone: Email:	Project Engineer: Telephone: Email:
Design Engineer: Telephone: Email:	Design Engineer: Telephone: Email:
Account Manager: Telephone: Email:	Account Manager: Telephone: Email:
Systems Engineer: Telephone: Email:	Systems Engineer: Telephone: Email:

Equipment Floor Plan (sample)

Location	Details
Floor	
Room	
Suite	
Position	
Rack No.	

Tools Required (sample)

Item No.	Item
1.	PC with Teraterm, 100BaseT interface, FTP Server and TFTP client applications
2.	Console port cable
3.	Ethernet cable

Implementation Task List (sample)

Step No.	Task
1.	Connect to the router
2.	Verify the current installation and create backup file
3.	Change IOS version (on all routers)
4.	Update IP address configuration (on distribution routers)
5.	Configure EIGRP routing protocol
6.	Verify configuration and record the results

Modely návrhu sietí – záverečné poznámky

- Vytvorením implementačného plánu a jeho realizáciou sa zaoberajú aj iné uvedené metodiky
 - ITIL je suma tzv. best practices, vytvorenie implementačného plánu a jeho realizáciu obsahuje ako jednu zo svojich súčastí
 - FCAPS obsahuje vytvorenie implementačného plánu a jeho realizáciu v kategórii Configuration management
 - TMN je podobný FCAPS-u, implementačný plán a jeho realizácia sú súčasťou stavebných blokov v TMN
- Všetky tieto modely predstavujú **štruktúrovaný** prístup k rozširovaniu siete a riešeniu problémov
 - Opakom je tzv. **ad-hoc prístup**, ktorý je vhodný pre malé siete, avšak vo väčších môže viesť k veľmi zásadným problémom
 - „Vykonaj zmenu len keď ju treba“

Ďalšie odkazy

- <http://cisco.com/go/sona>
 - Service-Oriented Network Architecture
- <http://cisco.com/go/lifecycle>
 - Cisco Lifecycle Services
- <http://cisco.com/go/safe>
 - SAFE Blueprint
- <http://cisco.com/go/cvd>
 - Cisco Validated Design
- <http://cisco.com/go/borderless>
 - Cisco Borderless Networks

Základy smerovania v IPv4 sieťach



Protokol IP

- Základným protokolom súčasných sietí je protokol IP
 - V súčasnosti sa používa verzia 4, RFC 791 a mnohé ďalšie
 - O verzii 6 bude pojednanie v samostatnej kapitole
- Protokol IP zabezpečuje
 - Logické adresovanie sietí a staníc v nich
 - Prostriedky pre doručovanie paketov medzi koncovými uzlami
 - Best-effort delivery
- V IPv4 má každé sieťové rozhranie samostatnú adresu
 - Zariadenie má toľko adries, koľkými rozhraniami komunikuje
- IPv4 adresa: 4B, zapísané ako štyri oktety oddelené bodkou

IPv4 sieťová adresa

- Každá sieťová adresa má dve časti:
 - **Identifikátor siete** (predčíslenie, prefix, network part, net ID)
 - **Identifikátor počítača** v danej sieti (číslo, host part, host ID)
 - Prirodzená analógia s inými hierarchicky štruktúrovanými číslami, napr. PSČ alebo telefónnymi číslami
- Smerovanie v ľubovoľnom L3 protokole sa zaoberá identifikátormi sietí (predčísliami)
 - Pre smerovanie nie je číslo konkrétneho počítača zaujímavé:
 - ak sme dopravili paket na okraj cieľovej siete, o zvyšok sa postará L2 (susedné stanice)
 - Jedna IP sieť je jedna broadcastová doména
 - Všetky stanice v spoločnej IP sieti sa považujú za susedné,
 - t.j. sú schopné komunikovať bezprostredne, priamo medzi sebou cez L2 technológiu

Predčíslenie siete (identifikátor siete)

- Veľkosť predčíslenia siete v IP adrese je premenlivá
- Viaceré spôsoby, ako z IP adresy zistiť predčíslenie:
 - Prvý prístup: prvý oktet je predčíslenie, zvyšok je číslo počítača
 - Druhý prístup: triedy IP adries (A, B, C, D, E)
 - Tretí prístup: zavedenie sieťovej masky (CIDR, VLSM)
- Keďže veľkosti predčíslí sú premenlivé, zaviedol sa pojem „*adresa siete*“, ktorá má vždy rovnakú dĺžku – 4B
 - Predčíslenie siete doplnené nulami na veľkosť IP adresy (4B)
 - Adresa siete: numericky najnižšie číslo s daným predčíslím
 - Broadcast: numericky najvyššie číslo s daným predčíslím
- Základné smerovanie v IPv4 sa riadi **adresami cieľových sietí** (t.j. nie odosielateľom či inými parametrami)

(Sub)Sieťová maska

- Identifikácia bitov predčísčia z adresy siete
- Význam bitov sieťovej masky:
 - Ak je n-ty bit v maske nastavený na
 - 1: n-ty bit v IP adrese patrí do predčísčia
 - 0: n-ty bit v IP adrese patrí do čísla stanice

158	193	138	40
10011110	11000001	10001010	00101000
11111111	11111111	11111111	00000000

- Elementárna binárna operácia AND priamo z IP adresy a masky vypočíta IP adresu príslušnej siete

(Sub)Sieťová maska

- Hranice medzi predčísľím siete a číslom počítača nemusia byť na hraniciach bajtov
- Výsledné IP čísla sietí teda nemusia po prepočte do desiatkovej sústavy končiť 0

$$158.193.138.40 \text{ \& } 255.255.255.224 = 158.193.138.32$$

10011110	11000001	10001010	00101000
AND			
11111111	11111111	11111111	11100000
=			
10011110	11000001	10001010	00100000

Smerovanie v IP

■ Smerovanie

- Je proces zisťovania a výberu ďalšej cesty pre paket smerom k cieľu na základe informácií v hlavičke smerovaného paketu a znalosti smerovača
 - Informácia = cieľová IP adresa
- Zoznam cieľových sietí, ktoré smerovač pozná, si uchováva v smerovacej tabuľke
 - Vo forme smerovacích informácií (položiek)
 - Cieľová sieť a jej maska
 - IP adresa ďalšieho smerovača (next hop) na ceste
 - Pre IGP: adresa susedného smerovača
 - Pre EGP: adresa okrajového smerovača AS domény
 - Ďalšie informácie o položke

Budovanie smerovacej tabuľky

- Smerovač defaultne vie len o priamo pripojených sieťach
- O vzdialených sieťach sa musí „nejako“ dozvedieť „z vonku“
- Tieto informácie môže smerovač získať
 - **Staticky**
 - Budovaná a udržiavaná manuálnym pridávaním statických smerovacích ciest administrátorom siete
 - **Dynamicky**
 - Budovaná a aktualizovaná použitím smerovacích protokolov
 - **Cisco On-Demand Routing (ODR)**
 - Poskytuje menšie zaťaženie ako dynamické smerovanie a menej konfigurácie ako statické smerovanie

show ip route

<output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

172.16.0.0/24 is subnetted, 4 subnets

R 172.16.1.0 [120/1] via 172.16.2.1, 00:00:00, Serial0/0/0

C 172.16.2.0 is directly connected, Serial0/0/0

C 172.16.3.0 is directly connected, FastEthernet0/0

C 192.168.1.0/24 is directly connected, Serial0/0/1

S* 0.0.0.0/0 is directly connected, Serial0/0/1

Smerovacia tabuľka – umiestňovanie záznamov

- Sieť (smerovací záznam) bude do smerovacej tabuľky umiestnená len pri splnení týchto predpokladov:
 1. Ak je cieľová sieť priamo pripojená,
 - potom rozhranie do tejto siete musí byť v stave „*up, line protocol up*“
 2. Ak je cieľová sieť dostupná cez istý next hop, potom musí byť možné rekurzívnym vyhľadáním tohto next hop-u zistiť výstupné rozhranie
 - Kvôli ochrane sa default route **nikdy nepoužije** na vyhľadanie next hop adresy
 - Inými slovami, každý záznam v smerovacej tabuľke musí viesť (po prípadnom rekurzívnom vyhľadaní) na živé výstupné rozhranie
- Kedykoľvek prestane byť niektorá z týchto požiadaviek splnená
 - daná cieľová sieť bude zo smerovacej tabuľky **odstránená!**

Rekurzívne záznamy v smerovacej tabuľke

```
R1# show ip route
```

```
Gateway of last resort is not set
```

```
    10.0.0.0/24 is subnetted, 1 subnets
```

```
C    10.0.0.0 is directly connected, Serial1/0
```

```
S    11.0.0.0/8 [1/0] via 10.0.0.2
```

```
S    12.0.0.0/8 [1/0] via 11.0.0.2
```

```
S    13.0.0.0/8 [1/0] via 12.0.0.2
```

```
S    14.0.0.0/8 [1/0] via 13.0.0.2
```

```
R1# configure terminal
```

```
R1(config)# no ip route 12.0.0.0 255.0.0.0
```

```
R1(config)# do show ip route
```

```
Gateway of last resort is not set
```

```
    10.0.0.0/24 is subnetted, 1 subnets
```

```
C    10.0.0.0 is directly connected, Serial1/0
```

```
S    11.0.0.0/8 [1/0] via 10.0.0.2
```

```
R1(config)#
```

Smerovacia tabuľka

- IP smerovacia tabuľka nemá možnosť uložiť celú trasu do cieľa
- Smerovacia tabuľka je interne usporiadaná **zostupne** podľa masky
 - Za účelom zrýchlenia prehľadávania pri smerovaní
 - Záznamy sú usporiadané od najkonkrétnejších po menej detailné
- Smerovacia tabuľka môže obsahovať (a často obsahuje) siete, ktoré sa vzájomne prekrývajú
 - Použije sa prvá najšpecifickejšia zhoda (Best Match/Longest Match)
- Za istých podmienok môže smerovacia tabuľka obsahovať **tú istú cieľovú sieť** niekoľkokrát
 - „Tá istá sieť“ znamená zhodu v dvojici [Sieť, Maska]
 - Spôsob realizácie load balancingu

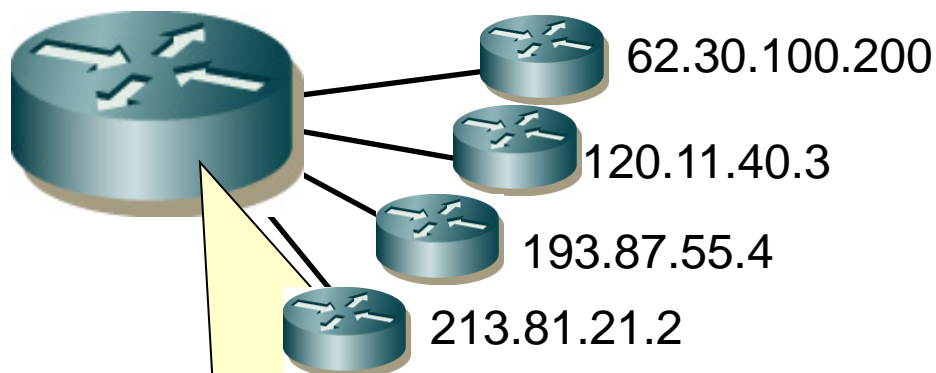
Činnosť smerovača pri smerovaní

IP Packet Destination	172.16.0.10	10101100.00010000.00000000.00001010
Route 1	172.16.0.0/12	10101100.00010000.00000000.00000000
Route 2	172.16.0.0/18	10101100.00010000.00000000.00000000
Route 3	172.16.0.0/26	10101100.00010000.00000000.00000000

Longest Match to IP Packet Destination 

- Smerovač využíva operáciu AND na to, aby zo svojho pohľadu určil cieľovú sieť príjemcu
- Vyhľadáva sa čo najšpecifickejšia cieľová sieť
 - Tzv. longest prefix match or best match
 - Súčin cieľovej IP adresy a masky daného smerovacieho záznamu
- Pri smerovaní je vhodné vedieť, že
 - Smerovač sa rozhoduje sám pre seba
 - Rozhodovanie sa opakuje na každom smerovači nezávisle
 - Rozhodnutie o ceste v jednom smere nič nehovorí o ceste nazad
 - Na jednej strane nevýhoda kvôli opakovanej činnosti, na strane druhej veľký význam pre hierarchiu v smerovaní (sumarizácia, agregácia ciest)

Základy smerovania v IPv4



87.197.31.42 & 255.255.255.248 =

87.197.31.40

87.197.31.36 & 255.255.255.240 =

87.197.31.32

87.197.1.1 & 255.255.0.0 =

87.197.0.0

213.81.187.59 & 0.0.0.0 =

0.0.0.0

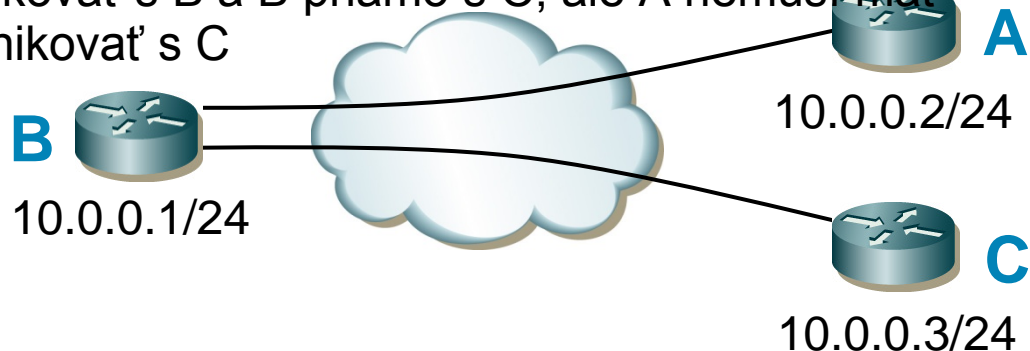
Maska	Cieľová sieť	Next hop
255.255.255.248	87.197.31.40	62.30.100.200
255.255.255.240	87.197.31.32	120.11.40.3
255.255.0.0	87.197.0.0	193.87.55.4
0.0.0.0	0.0.0.0	213.81.21.2

Smerovacia tabuľka – Next hop IP

- IP adresy next-hop smerovačov sú využité pre vyhľadanie ich fyzickej (L2) adresy v ARP, InvARP, dialer mapping resp. inej tabuľke
 - Nikdy sa nevyužívajú v hlavičke samotného IP paketu, pokiaľ nasledujúci smerovač nie je koncovým adresátom!
 - Pozor na rekurzívny lookup!
- Za istých okolností je možné v smerovacej tabuľke sa odkázať len na výstupné rozhranie bez informácie o next-hop smerovači
 - Vhodné **len pri point-to-point rozhraniach**
 - Pri multiaccess rozhraniach môžu vzniknúť problémy
 - BMA
 - NBMA

Špecifiká NBMA sietí

- Špeciálny prípad tvoria tzv. NBMA siete
 - Non-Broadcast:
 - Linková technológia nemá prostriedky na doručovanie broadcastov.
 - Odosielateľ musí zabezpečiť ich distribúciu vo vlastnej réžii.
 - Realizované spravidla virtuálnymi okruhmi, ktoré majú point-to-point povahu
 - ATM, X.25, Frame Relay, Dynamic Multipoint VPN
 - Multi-Access:
 - Cez jedno rozhranie smerovača sú potenciálne dostupné **mnohé** ďalšie smerovače **v tej istej IP sieti**
 - Problém: Nemusí byť zaručená tzv. tranzitivita
 - A môže priamo komunikovať s B a B priamo s C, ale A nemusí mať možnosť priamo komunikovať s C



Špecifiká NBMA sietí

- Na NBMA sieťach je potrebné zvážiť, kto s kým môže priamo komunikovať
- Viaceré smerovacie protokoly vyžadujú pre správnu činnosť nad NBMA sieťami dodatočnú konfiguráciu
 - Korekcia split-horizon pravidla
 - Vymenovanie priamo pripojených susedov
 - Korekcia next-hop smerovačov
 - Ovplyvnenie volieb DR/BDR (pri OSPF)

Prehľadávanie smerovacej tabuľky – bližší pohľad (neplatí pre CEF)

- Smerovacia tabuľka cisco smerovačov je hierarchicky organizovaná do
 - Level 1 routes
 - Majú subnet masku rovnú alebo kratšiu ako classfull masku adresy siete
 - Supernet routes, default r., network routes
 - Level 2 routes
 - Majú subnet masku dlhšiu ako classfull masku adresy siete

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

172.16.0.0/24 is subnetted, 4 subnets

Level one

R 172.16.1.0 [120/1] via 172.16.2.1, 00:00:00, Serial0/0/0

Level two

C 172.16.2.0 is directly connected, Serial0/0/0

C 172.16.3.0 is directly connected, FastEthernet0/0

C 192.168.1.0/24 is directly connected, Serial0/0/1

S* 0.0.0.0/0 is directly connected, Serial0/0/1

Level one

Vzťah level 1 a level 2 a ultimatívne cesty

■ Parent a Child Routes

- **Parent route** je cesta **level 1**
 - Neobsahuje informácie o next hop IP adrese alebo výstupnom rozhraní
- **Child route** je cesta **level 2**
 - Je **subnet** danej classfull/classless siete

Parent route

Child route

```
172.16.0.0/24 is subnetted, 4 subnets
R    172.16.1.0 [120/1] via 172.16.2.1, 00:00:00, Serial0/0/0
C    172.16.2.0 is directly connected, Serial0/0/0
C    172.16.3.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

■ Obe úrovne ciest (L1 a L2) môžu byť ultimatívne (ultimate)

- Ak obsahujú informáciu o preposlaní paketu
 - Next hop IP adresu alebo výstupné rozhranie

```
172.16.0.0/24 is subnetted, 4 subnets
R    172.16.1.0 [120/1] via 172.16.2.1, 00:00:00, Serial0/0/0
C    172.16.2.0 is directly connected, Serial0/0/0
C    172.16.3.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

Ultimate
routes

Prehľadávanie smerovacej tabuľky

- Dva typy správania pri prehľadávaní smerovacej tabuľky
 - **Ip classless vs Ip classful**
- Proces prehľadávania tabuľky bude
 - **Prehľadaj level 1 cesty**
 - Ak je nájdená najlepšia zhoda, cesta je ultimatívna a nie je rodičovská, použi ju na poslanie paketu
 - **Prehľadaj level 2 (child) cesty**
 - Ak je nájdená najlepšia zhoda na L2 child ceste, použi ju na poslanie paketu
 - Ak nie je nájdená zhoda na L2 – zisti typ smerovacieho správania
 - IP classless vs. ip classfull
 - **Ďalší krok podľa typu správania**
 - Ak je použité *classful*, paket je dropnutý
 - Ak je použité *classless*, smerovač prehľadá zvyšné L1 cesty
 - Ak existuje L1 superroute alebo default route, použije ju na preposlanie paketu
 - Ak nie je, paket je dropnutý

Routing Behavior – ip classless

- **IP classless routing behavior** in effect then
 - Search level 1 routes
 - If a match exists and is ultimate then forward packet (ultimate route)
 - If L1 is not ultimate, check L2 child routes
 - If there is no match check the rest of L1 routes
 - If match or def. route exist
 - Forward packet
 - If not, packet is dropped

show ip route

<output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

172.16.0.0/24 is subnetted, 4 subnets

R 172.16.1.0 [120/1] via 172.16.2.1, 00:00:00, Serial0/0/0

C 172.16.2.0 is directly connected, Serial0/0/0

C 172.16.3.0 is directly connected, FastEthernet0/0

C 192.168.1.0/24 is directly connected, Serial0/0/1

S* 0.0.0.0/0 is directly connected, Serial0/0/1

- Routing for network 172.16.4.0/24
- No child route, try other L1,
 - here def. route is used

Routing Behavior – ip classfull

- **IP classfull routing behavior** in effect then
 - Search level 1 routes
 - If a match exists and is ultimate then forward packet (ultimate route)
 - If L1 is not ultimate, check L2 child routes
 - If there is no match drop packet
- **Command**
 - **no ip classless**

show ip route

<output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

172.16.0.0/24 is subnetted, 4 subnets


R 172.16.1.0 [120/1] via 172.16.2.1, 00:00:00, Serial0/0/0

C 172.16.2.0 is directly connected, Serial0/0/0

C 172.16.3.0 is directly connected, FastEthernet0/0

C 192.168.1.0/24 is directly connected, Serial0/0/1

S* 0.0.0.0/0 is directly connected, Serial0/0/1



Routing for
network
172.16.4.0/24
No L2 route,
packet is dropped

Základy smerovania v IPv4

- Odporúčané dokumenty:
 - Doc ID 8651: „Route Selection in Cisco Routers“
 - Doc ID 5212: „How Does Load Balancing Work?“
 - Doc ID 16448: „Configuring a Gateway of Last Resort Using IP Commands“

Statické smerovanie



Statické smerovanie

- Základ každého smerovania
- Obsah smerovacej tabuľky stanovuje administrátor
- Vhodné použiť ak:
 - Chceme mať absolútnu kontrolu nad smerovacími cestami, ktoré bude smerovač používať
 - Ak chceme riešiť backup k dynamickým cestám
 - Ak je neželané nasadenie dynamických smerovacích protokolov
 - Napr. nad pomalými linkami
 - Ak riešime dosiahnuteľnosť tzv. stub networks
 - Napr. pri hub and spoke

Konfigurácia statického smerovania

```
Router(config)# ip route prefix mask address interface dhcp distance  
name next-hop-name permanent track number tag tag
```

Parameter	Description
<i>prefix mask</i>	The IP network and subnet mask for the remote network to be entered into the IP routing table.
<i>address</i>	The IP address of the next hop that can be used to reach the destination network.
<i>interface</i>	The local router outbound interface to be used to reach the destination network.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3).
<i>distance</i>	(Optional) The administrative distance to be assigned to this route.
name <i>next-hop-name</i>	(Optional) Applies a name to the specified route.
permanent	(Optional) Specifies that the route will not be removed from the routing table even if the interface associated with the route goes down.
track <i>number</i>	(Optional) Associates a track object with this route. Valid values for the number argument range from 1 to 500.
tag <i>tag</i>	(Optional) A value that can be used as a match value in route maps.

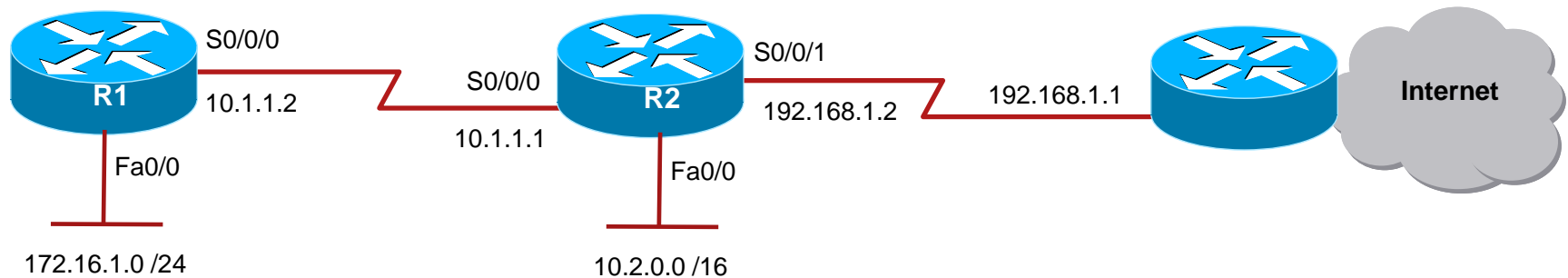
Použitie výstupného rozhrania v príkaze ip route

- Využívanie len výstupného rozhrania v statických cestách bez uvedenia IP adresy next-hop sa odporúča len pre point-to-point linky
 - Pri iných typoch môže viesť k nepríjemnostiam
 - Napr. na multiaccess sieťach smerovač nevie adresu suseda, ktorému packet posunúť
 - Ethernet
 - Pre každú IP adresu príjemcu smerovač konzultuje svoju ARP cache
 - Ak sa príjemca v cache nenachádza, smerovač generuje ARP Request a očakáva ARP Response
 - Ak sa mapovanie IP/MAC nepodarí zistiť, paket sa zahodí
 - Veľký ARP traffic, veľká ARP cache
 - Činnosť je závislá od aktívnej služby **ProxyARP** na susedných smerovačoch
 - Multipoint Frame Relay
 - Pre každú IP adresu príjemcu smerovač konzultuje svoju IP/DLCI map tabuľku
 - Paket pre nemapovaného príjemcu sa zahodí
 - Nie je možnosť opýtať sa na konkrétne mapovanie

Použitie IP adresy next hop v príkaze ip route

- Využívanie len IP adresy next-hop môže byť neoptimálne
 - Rekurzívny lookup
- +
- Ethernet
 - Pre každú IP adresu príjemcu (tu suseda) smerovač konzultuje svoju ARP cache
 - Ak sa príjemca v cache nenachádza, smerovač generuje ARP Request a očakáva ARP Response
 - Ak sa mapovanie IP/MAC nepodarí zistiť, paket sa zahodí
 - Veľký ARP traffic, veľká ARP cache
- Pre multicaccess siete sa odporúča použiť kombináciu výstupné rozhranie a IP adresa next-hop

Konfigurácia defaultnej statickej cesty



- R2 je konfigurované so statickou cestou na R1 LAN a default cestou pre internet

```
R2(config)# ip route 172.16.1.0 255.255.255.0 s0/0/0
R2(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

- R1 je konfigurovaný len s default cestou

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1
R1(config)# exit
R1# show ip route

<output omitted>
Gateway of last resort is not set
C    172.16.1.0 is directly connected, FastEthernet0/0
C    10.1.1.0 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 10.1.1.1
R1#
```

Statické smerovanie

■ Výhody

- Žiadne zaťaženie smerovača pri budovaní smerovacích tabuliek
- Žiadne vymieňané sieťové dáta
 - Šetrí sa prenosová kapacita siete
- Bezpečnosť
 - Smerovač neposiela smerovacie updates
 - Nie je možné odchytiť dáta a rekonštruovať topológiu siete
 - Nie je možné podstrčiť chybné smerovacie informácie
- Predpovedateľnosť
 - Administrátor presne kontroluje smerovanie smerovača

■ Nevýhody

- Vysoká náročnosť na údržbu
 - Administrátor musí všetko ručne nastaviť
- Slabá adaptabilita na zmeny v sieti



Dynamické smerovanie



Dynamické smerovanie –

Pár faktov o smerovacích protokoloch

- Dynamické smerovanie (RIPv1, RIPv2, EIGRP, OSPF, a IS-IS) umožňuje smerovaču automaticky sa prispôsobiť topologickým zmenám
 - Vďaka použitiu **dynamických smerovacích protokolov**
- Cieľ smerovacích protokolov
 - Naplniť smerovaciu tabuľku zoznamom dosiahnuteľných sietí a určiť najvhodnejšie cesty do nich
- Naplnenie smerovacej tabuľky sa udeje ako výsledok behu algoritmu daného smerovacieho protokolu nad jeho pracovnou databázou
 - Smerovacie protokoly majú spravidla vlastné pracovné databázy, ktoré nie sú totožné so smerovacou tabuľkou
 - Pracovné databázy rôznych smerovacích protokolov nie sú vzájomne medzi nimi zdieľané
 - Oddelená výkonná a riadiaca časť
- Smerovací protokol rozposiela do okolia
 - priamo pripojené siete vymenované príkazmi **network**
 - Rozhranie musí byť up, up
 - ostatné siete, o ktorých sa tým istým protokolom naučil od susedov

Pár faktov o smerovacích protokoloch

- Každý smerovací protokol do smerovacej tabuľky umiestňuje dosiahnuteľnú cieľovú sieť s najnižšou metrikou (Best Route)
 - Metrika je teda kritériom, podľa ktorého sa smerovací protokol rozhoduje, ktorá cesta je najvhodnejšia
- Na smerovači môže bežať viacero smerovacích protokolov naraz
 - Metriky medzi rôznymi protokolmi sa nedajú medzi sebou porovnávať, lebo sú kalkulované úplne odlišne
- Preto Cisco zavádza pojem „**administrative distance**“
 - Dá sa označiť aj ako (ne)dôveryhodnosť informácie o sieti – ako ďaleko je informácia „od pravdy“
 - Čím nižšia administratívna vzdialenosť, tým dôveryhodnejšia informácia
- Ak existuje viacero zdrojov informácie o tej istej sieti, ktoré spĺňajú podmienky na vloženie do smerovacej tabuľky
 - Najprv sa vyhodnocuje administratívna vzdialenosť
 - Až potom sa vyhodnocuje metrika

Administratívna vzdialenosť

Typ informácie	Administratívna vzdialenosť
Priamo pripojená sieť	0
Staticky vložená informácia	1
EIGRP sumárna položka	5
BGP sieť z iného AS	20
EIGRP interná sieť	90
OSPF	110
IS-IS	115
RIP	120
ODR	160
EIGRP externá sieť	170
BGP sieť z toho istého AS	200
DHCP	254
Absolútne nedôveryhodný zdroj	255

Load balancing

- Smerovací protokol môže do smerovacej tabuľky umiestniť viacero záznamov o tej istej cieľovej sieti
 - Typicky ak majú identickú (a najnižšiu) metriku
 - EIGRP môže vložiť aj smery s rôznou metriku
- Pokiaľ sú v smerovacej tabuľke viaceré záznamy o tej istej sieti, využijú sa pre *load balancing*
 - O jednej sieti smie byť v smerovacej tabuľke najviac 16 záznamov (obmedzenie smerovacej tabuľky)
 - Toto maximum sa môže meniť v závislosti od platformy a od verzie IOSu
 - IGP protokoly majú implicitne prednastavený limit na 4 záznamy pre danú sieť (dodatočná ochrana)
 - Zmena príkazom **maximum-paths**
 - Protokol BGP má implicitne nastavený limit na 1

Klasifikácia smerovacích protokolov

- Princípy smerovacích algoritmov:
 - Distance-Vector (RIP, EIGRP)
 - Smerovače si vymieňajú zoznam cieľových sietí a svojich najlepších vzdialeností do nich
 - Správy: vektory (t.j. polia) vzdialeností
 - Path-Vector (BGP)
 - Smerovače si vymieňajú zoznam cieľových sietí a popis cesty od seba do cieľovej siete (napr. zoznam tranzitných AS)
 - Správy: vektory (t.j. polia) atribútov
 - Link-State (OSPF, IS-IS)
 - Smerovače si vymieňajú informácie pre vytvorenie grafovej reprezentácie siete
 - Správy: popisy prepojení

Distance vector vs Link-state

■ Distance vector

- Obmedzené poznanie topológie siete
- Používa časté, periodické zasielanie smerovacích tabuliek medzi susedmi
- Pomalá konvergencia
- Náchylný na vznik slučiek
 - Split, poisoning, max. count, hold down timers, event driven updates
- Jednoduchá konfigurácia
- Nízke nároky na hardvér smerovača
- Pomerne vysoká spotreba prenosových kapacít siete

■ Link state

- Všeobecná znalosť celej topológie siete
- Používa udalosťami spúšťané šírenie updates
- Updates šírené záplavovo
- Rýchla konvergencia
- SPF strom je bez slučkový
- Náročnejší na konfiguráciu
- Vysoké nároky na hardvér smerovača
- Menšia spotreba prenosových kapacít siete

Dynamické smerovanie

■ Výhody

- Vysoká adaptabilita
 - Schopnosť prispôbiť sa vzniknutým zmenám
- Nízka údržbová a konfiguračná náročnosť
 - Po krátkej konfigurácii pracujú samostatne

■ Nevýhody

- Zvýšené zaťaženie procesora
 - Generovanie updates
 - Spracovávanie updates
- Zvýšená spotreba systémových zdrojov
 - Udržovanie rôznych tabuliek v RAM
- Zvýšené využitie prenosových kapacít siete
 - Na prenos a príjem updates

Classful vs. Classless smerovací protokol

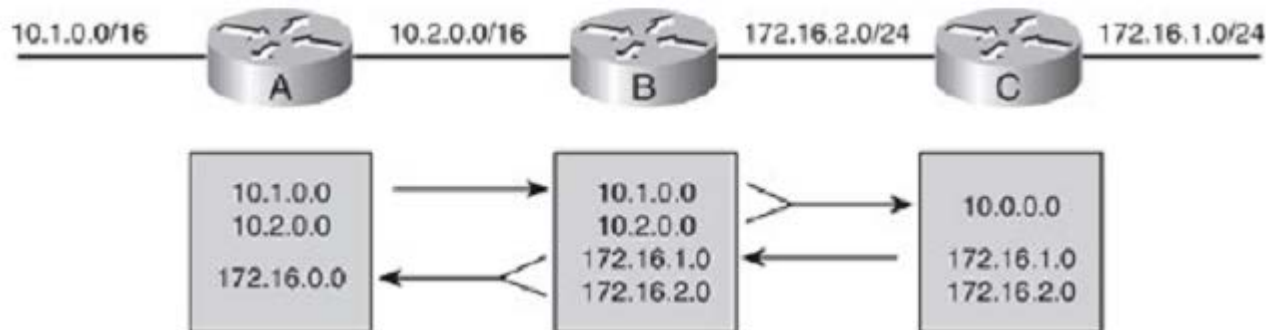
■ Classful Routing Protocol:

- Nepodporujú VLSM.
- Smerovacie aktualizácie neobsahujú subnet mask.
- Subnety iných sietí nie sú preposielané cez rozhrania iných sietí
 - Sumarizácia
- Discontiguous subnets nie sú viditeľné navzájom
- RIPv1, IGRP

■ Classless Routing Protocol:

- Podporujú VLSM.
- Smerovacie updates obsahujú subnet mask.
- Subnety iných sietí nie sú preposielané cez rozhrania iných sietí
 - Viac ďalší slajd
- Discontiguous subnets sú viditeľné navzájom
- RIPv2, EIGRP, OSPF, IS-IS, BGP

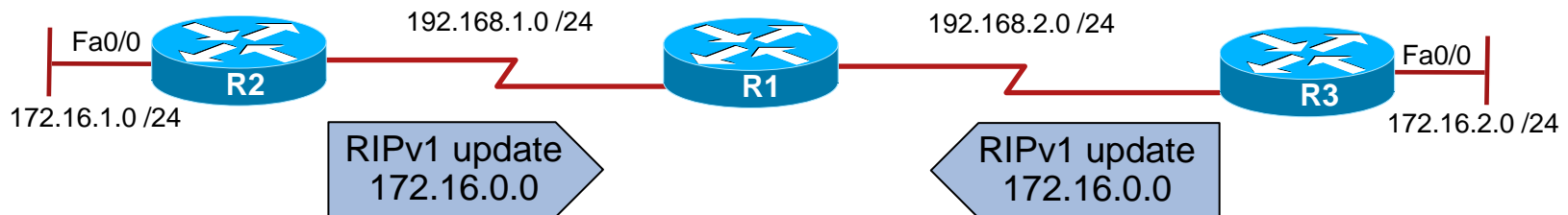
Route summarization



- **Classful** routing automatically summarize to the classful network boundary at major network boundaries
 - Smaller routing tables, smaller updates
- **Classless** routing protocols either do not automatically summarize or automatically summarize but this feature can be disabled.
 - OSPF or IS-IS do not support automatic network summarization.
 - RIPv2 and EIGRP perform automatic network summarization to maintain backward compatibility with RIPv1 and IGRP.
 - However, automatic summarization can be disabled in RIPv2 and EIGRP by using the **no auto-summary** router config command

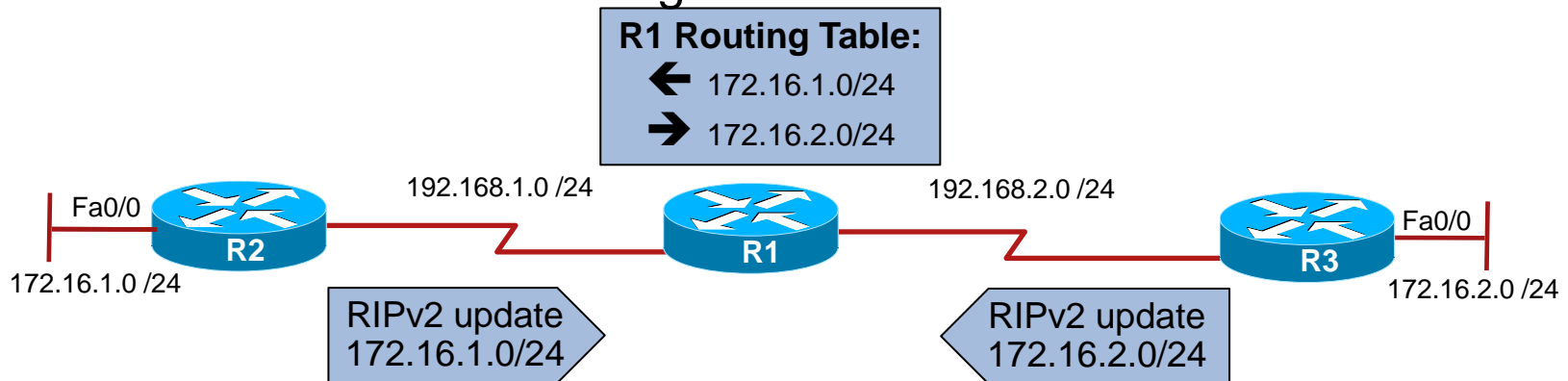
Discontiguous Subnets - Classful Routing

- Classful routing protocols do not support discontiguous networks.
- Discontiguous subnets are subnets of the same *major network* that are separated by a different major network.
 - For example, RIPv1 has been configured on all three routers.
 - Routers R2 and R3 advertise 172.16.0.0 to R1.
 - They cannot advertise the 172.16.1.0 /24 and 172.16.2.0 /24 subnets across a different major network because RIPv1 is classful.
 - R1 therefore receives summarized routes about 172.16.0.0 /16 from two different directions and it might make an incorrect routing decision.



Discontiguous Subnets - Classless Routing

- Classless routing protocols support discontiguous networks.
 - For example, RIPv2 has been configured on all three routers
 - Summary Off
 - Because of RIPv2, routers R2 and R3 can now advertise the 172.16.1.0 /24 and 172.16.2.0 /24 subnets across a different major network.
 - R1 therefore receives routes with valid subnet information and can now make a correct routing decision.



Charakteristiky smerovacích protokolov

Characteristics	RIPv1	RIPv2	EIGRP	IS-IS	OSPF	BGP
Distance vector	✓	✓	✓			✓
Link-state				✓	✓	
Classless		✓	✓	✓	✓	✓
VLSM support		✓	✓	✓	✓	✓
Automatic route summarization	✓	✓ (can be disabled using no auto-summary)	✓ (can be disabled using no auto-summary)			✓
Manual route summarization		✓	✓	✓	✓	✓
Hierarchical topology required				✓	✓	
Size of network	Small	Small	Large	Large	Large	Very large
Metric	Hops	Hops	Composite metric	Metric	Cost	Path attributes
Convergence time	Slow	Slow	Very fast	Fast	Fast	Slow

Routing Protocol Specifics

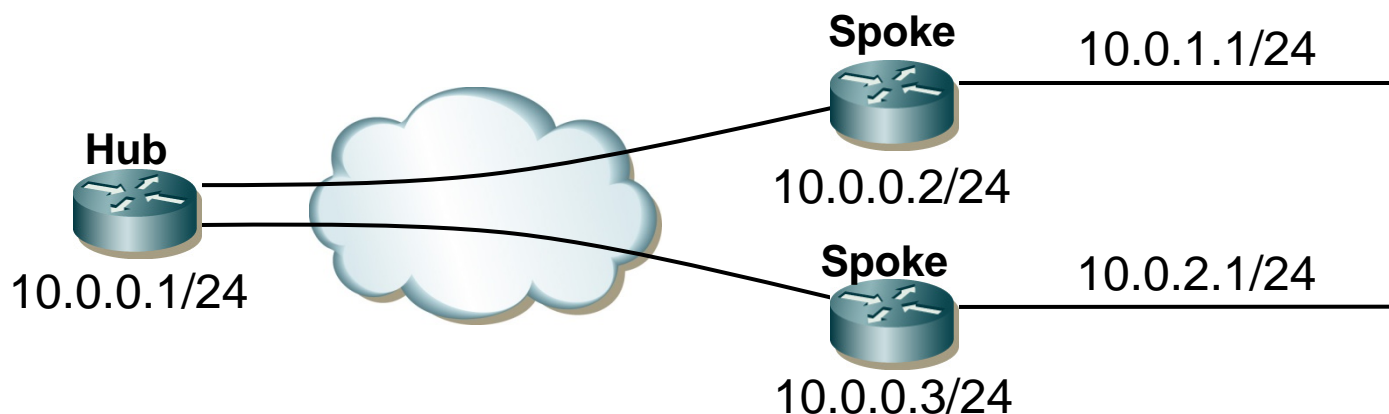
Routing Protocol	Protocol Number	Port Number	Admin Distance
RIP	--	UDP 520	120
IGRP	9	--	100
EIGRP	88	--	90 Summary Routes – 5 Redistributed Routes – 170
OSPF	89	--	110
IS-IS	124	--	115
BGP	--	TCP 179	eBGP – 20 iBGP – 200

On-Demand Routing



On Demand Routing

- V mnohých aplikáciách je typické tzv. zapojenie hub-and-spoke
- Za spoke smerovačmi sa nachádzajú tzv. stub siete
- Pre spoke routery stačí default route
- Hub router potrebuje zoznam všetkých LAN zo stub smerovačov



On Demand Routing

- **Document ID: 13710, 13716**
- Cisco implementovalo obmedzenú smerovaciu schopnosť do CDP
- Hub router rozpošle na spoke routery default route
- Spoke routery automaticky pošlú hub routeru zoznam svojich priamo pripojených sietí
- ODR sa aktivuje **výlučne na hub routeri**
- Na **spoke** routeroch **nesmie** byť aktívny žiaden smerovací protokol
 - Na spoke routeroch sa teda nekonfiguruje ani ODR, ani nijaký iný smerovací protokol
- Konfigurácia:

```
Hub(config)# router odr
Hub(config-router)# network NETWORK
Hub(config-router)# network NETWORK
```

```
R1(config)# router odr
R1(config)# do show ip route
<output omitted>
10.0.0.0/8 is subnetted, 2 subnets
  10.0.1.0/24 [160/1] via 10.0.0.2, 00:00:23, Serial0/0/1
  10.0.2.0/24 [160/1] via 10.0.0.3, 00:00:03, Serial0/0/2
<output omitted>
```

On Demand Routing

- Do ODR nemožno redistribuovať žiadne cudzie smery
- Činnosť ODR je závislá na CDP
- Pozor na aplikáciu ODR nad Frame Relay
 - CDP je *vypnuté* by default na multipoint rozhraniach
 - CDP je *zapnuté* by default na point-to-point rozhraniach

Ladenie ODR

- Nastavenie ODR časovačov

- Router(config-router)# **timers basic** *update invalid holddown flush*

- Zmena ODR časovačov

- *Default:*

- *update: 90 seconds*

- invalid: 270 seconds*

- holddown: 280 seconds*

- flush: 630 seconds*

- Nastavenie CDP časovačov (def. je 60 sek.)

- Router(config)# **cdp timer**



Plavajúce cesty – Floating routes



Statické smerovanie

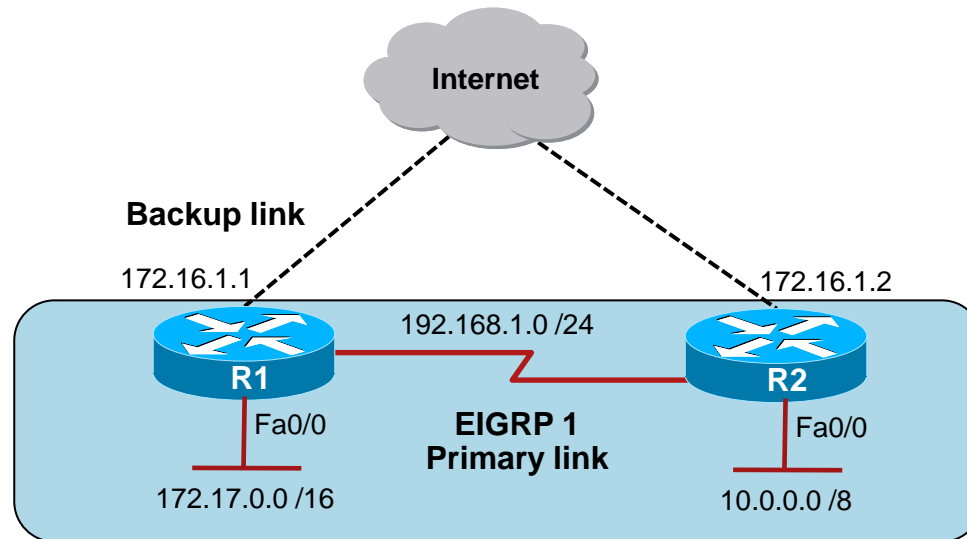
Floating Static Routes

- Statické smerovacie záznamy s vyššou AD
- Aktivujú sa v prípade, že neexistuje záznam s nižšou AD
- Typicky používané ako definície záložných trás pre dynamické cesty
 - AD záložnej statickej cesty je konfigurovaný vyšší ako AD primárnej cesty, info sa nereflektuje kým existuje primárna cesta
 - Pozor:
 - Ak má smerovač na výber statický záznam a informáciu zo smerovacieho protokolu s tou istou AD, uprednostní statický záznam
 - Statické záznamy majú internú metriku 0

Konfigurácia plávajúcej statickej cesty

Floating Static Route

- Statická cesta „pláva“ nad EIGRP cestou pre danú sieť
- Ak tá padne, záznam sa inštaluje do smerovacej tabuľky



```
R1(config)# ip route 10.0.0.0 255.0.0.0 172.16.1.2 100
R1(config)# router eigrp 1
R1(config-router)# network 172.17.0.0
R1(config-router)# network 192.168.1.0
```

```
R2(config)# ip route 172.17.0.0 255.255.0.0 172.16.1.1 100
R2(config)# router eigrp 1
R2(config-router)# network 10.0.0.0
R2(config-router)# network 192.168.1.0
```

Použitie masiek /31 na point-to-point linkách



Maska /31 na point-to-point linkách

- Sériové linky sú obvykle adresované s maskou /30
 - Je to však plytvanie – sériové linky majú spravidla iba dvojicu „koncov“ a pojem broadcastu nemá význam
- **RFC 3021** špecifikuje možnosť adresovať takéto spoje pomocou masky /31
 - Táto maska povoľuje dve adresy – práve pre dva konce
- Príklad:
 - 10.0.0.0/31 a 10.0.0.1/31
 - 192.0.2.254/31 a 192.0.2.255/31
- Možnosť používať masku /31 na sériových linkách je podporovaná od verzie IOSu 12.2(2)T
 - Konfiguruje sa úplne tradičným spôsobom

IP Unnumbered



IP Unnumbered

- Document ID: 13786
- Point-to-point rozhrania majú špecifickú povahu
 - Príjemca dát je jednoznačný – je na druhom konci kábla
 - Rozhranie by teoreticky nemuselo mať IP adresu
- IP Unnumbered: schopnosť point-to-point rozhraní „požičať“ si IP adresu iného rozhrania
 - Efektívnejšie využívanie IP adries
 - Cieľové siete v smerovacej tabuľke používajú priamo meno rozhrania ako špecifikáciu next-hop
- Nevýhody:
 - Činnosť rozhrania je závislá od stavu „master“ rozhrania, od ktorého je IP adresa vypožičaná (ideálne použiť Loopback rozhrania)
 - Unnumbered rozhranie nemožno testovať

IP Unnumbered

- Konfigurácia IP Unnumbered:

```
RTA(config)# int e0
RTA(config-if)# ip address 168.71.5.1 255.255.255.0
RTA(config-if)# no shut
RTA(config-if)# int s1
RTA(config-if)# ip unnumbered e0
```



By using IP unnumbered, serial interfaces can "borrow" an IP address from another interface.

RIPv2



Routing Information Protocol

- Typický predstaviteľ distance-vector protokolov
- V súčasnosti existujú 3 verzie
 - RIPv1: Historická, classful, RFC 1058
 - RIPv2: RFC 2453
 - RIPv6: RFC 2080
- Za svoju životaschopnosť vďaka svojej jednoduchosti, otvorenosti a širokej podpore
- Hoci sa možno stretnúť s názorom, že RIP je mŕtvý, nie je to pravda
 - Ideálny protokol pre malé nenáročné siete
 - Vynikajúci pre CE/PE výmeny informácií

Routing Information Protocol v. 2

Vlastnosti

- RIPv1 má nasledujúce vlastnosti:
 - Classful
 - Metrika: počet hopov
 - UDP/520, aktualizácie posielané periodicky každých 30 sekúnd ako tzv. limited broadcast na adresu 255.255.255.255
 - Maximálna metrika: 15 hopov
 - Classful správanie: [Document ID 13723](#)
- RIPv2 preberá väčšinu vlastností, kľúčové zmeny:
 - Classless
 - UDP/520, aktualizácie posielané periodicky každých 30 sekúnd ako multicast na 224.0.0.9
 - Autentifikácia
 - IP adresa odporúčaného next hop-u
 - Route tagging
 - Použité napr. pri redistribúcii

Zhody RIPv1 a RIPv2

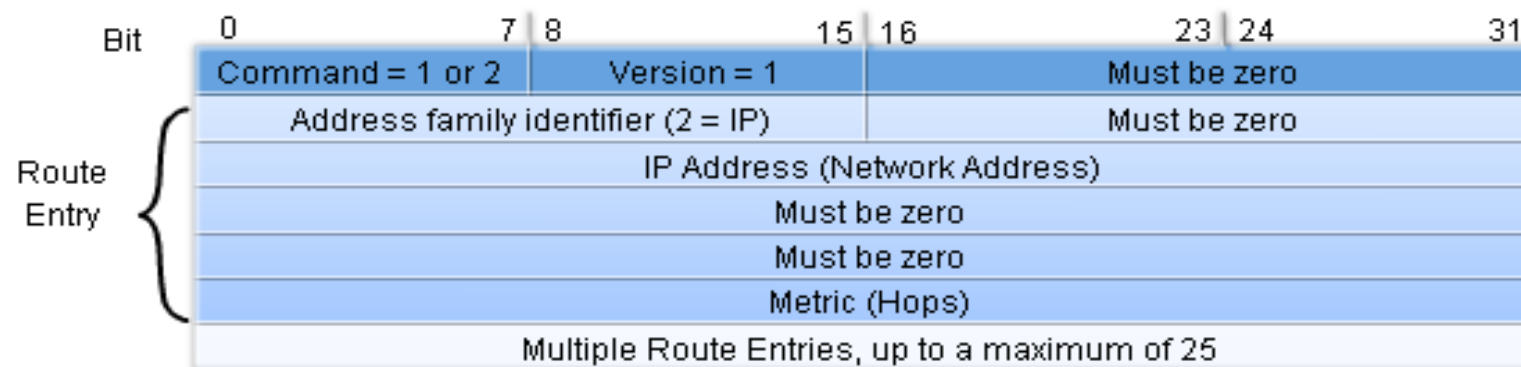
- Používajú tú istú metriku
- Používajú „*split horizon with poisson reverse*“
- Používajú udalosťami spúšťané zasielanie aktualizácií
- Rovnaké ohraničenie maxima
- Rovnaké periodické zasielanie updates každých 30s
- Používajú rovnaké časovače
 - Update, invalid, holddown, flush

Routing Information Protocol v. 2

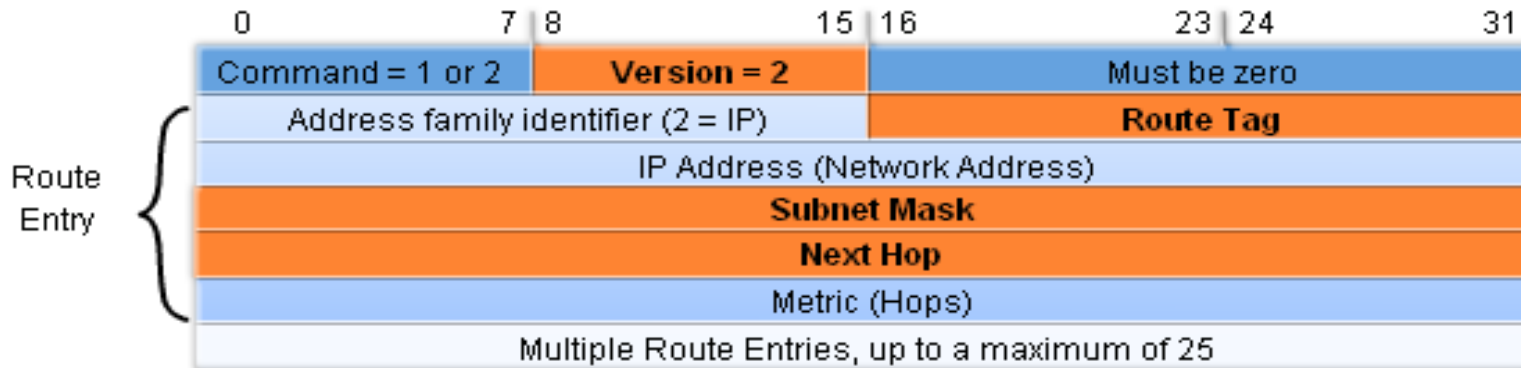
Formát paketu

- Porovnanie RIPv1 a RIPv2

RIPv1



RIPv2



Routing Information Protocol v. 2

Základná konfigurácia

- Základná konfigurácia:

```
Router(config)# router rip  
Router(config-router)# no auto-summary  
Router(config-router)# version 2  
Router(config-router)# network ...  
Router(config-router)# network ...
```

- Účel príkazu **network**:
 - Do ktorej priamo pripojenej siete posielame RIP pakety
 - Z ktorej priamo pripojenej siete prijímame RIP pakety
 - O ktorej priamo pripojenej sieti budeme v našich RIP paketoch ostatným smerovačom hovoriť
- Za priamo pripojenú sieť sa pre účely distance-vector protokolov považujú aj staticky definované smery, v ktorých je definované výstupné rozhranie bez next-hop IP

Routing Information Protocol v. 2

Generovanie default route

- RIP umožňuje distribuovať default route
- Generovanie default route do odosielaných RIP paketov na príslušnom smerovači:

```
Router(config)# router rip  
Router(config-router)# default-information originate
```

- Takto konfigurovaný smerovač generuje default route nezávisle od toho, či sám default route pozná alebo nie
- Tento príkaz patrí len na tie smerovače, ktoré skutočne spájajú našu sieť (autonómny systém) s iným AS
 - Týchto smerovačov môže byť viac
 - Vnútorne smerovače si vyberú najbližší hraničný smerovač
- Známa chyba IOSu: niekedy smerovače nechcú spustiť generovanie default route, potrebné:

```
Router# clear ip route *
```


Routing Information Protocol v. 2

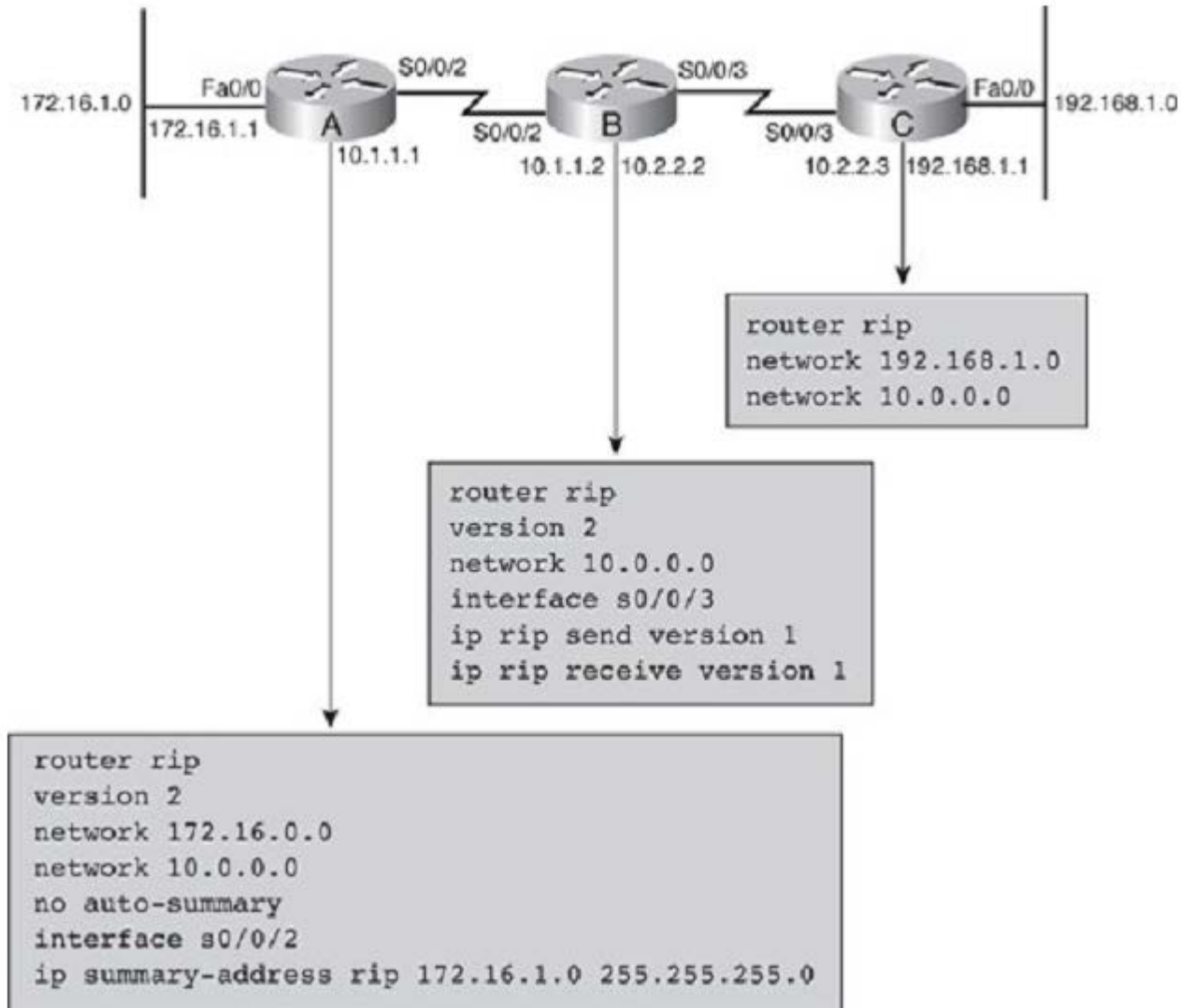
Spätná kompatibilita

- Spolupráca a spätná kompatibilita s RIPv1 smerovačmi
 - Bez príkazu „version“:
 - Posiela sa verzia 1
 - Prijíma sa verzia 1 aj 2
 - S príkazom „version“
 - Posiela aj prijíma sa len uvedená verzia
- Pokiaľ je potrebné na konkrétnom rozhraní zmeniť použitú verziu protokolu:

```
Router(config-if)# ip rip send version {1 | 2 | 1 2}  
Router(config-if)# ip rip receive version {1 | 2 | 1 2}
```

- Zmena zrejme platí na všetkých RIP susedov na danom rozhraní

Príklad konfigurácie a spolupráce RIPv1 a RIPv2



Routing Information Protocol v. 2

Autentifikácia

- RIP je protokol, ktorý slepo dôveruje informácii prichádzajúcej od niektorého zo susedov
 - Otvorená náruč pre podstrčenie zlomyseľnej informácie
- Ochrana: autentifikácia
 - Podpis každého paketu pomocou dohodnutého hesla
 - Dve formy:
 - Plaintext
 - MD5 hash
- Aktivácia autentifikácie
 - Vytvorenie „kľúčenky“ – zoznamu kľúčov
 - Aktivácia konkrétnej formy autentifikácie na rozhraní
 - Aktivácia konkrétnej kľúčenky na rozhraní

Routing Information Protocol v. 2

Konfigurácia autentifikácie

- Vytvorenie kľúčenky:

```
Router(config)# key chain MENO  
Router(config-keychain)# key ČÍSLO  
Router(config-keychain-key)# key-string HESLO
```

- Aktivácia konkrétnej formy autentifikácie na rozhraní:

```
Router(config-if)# ip rip authentication mode {md5|text}
```

- Aktivácia konkrétnej kľúčenky na rozhraní:

```
Router(config-if)# ip rip authentication key-chain MENO
```

Routing Information Protocol v. 2

Autentifikácia

- Názvy kľúčeniek sa môžu líšiť, avšak je potrebné, aby čísla kľúčov boli identické
 - Číslo kľúča použitého na podpis paketu sa vkladá do tohto paketu, aby bolo možné u príjemcu paket overiť zodpovedajúcim kľúčom
- Na uvedenie si: kľúčom na danom rozhraní sa podpisuje a overuje každý RIP paket
 - Ak je rozhranie pripojené na multiaccess sieť, musia všetky routery na spoločnom segmente používať identický kľúč
- Viaceré kľúče
 - Každý kľúč v kľúčenke má dvojicu časov platnosti
 - send-lifetime: platnosť kľúča na podpísanie odchádzajúcich správ
 - accept-lifetime: platnosť kľúča na overenie prijatých správ
 - Ak sú v kľúčenke viaceré kľúče platné pre odosielanie, bude sa využívať platný kľúč s **najnižším** číslom

Routing Information Protocol v. 2

Prechod na nový kľúč

- Odporúčaný postup pre prechod na nový kľúč:
 - V **prvom** kroku pridať na všetkých smerovačoch do kľúčenky nový kľúč so správnym heslom a vyšším číslom
 - Smerovače budú stále na odosielanie i prijímanie paketov používať starší kľúč s nižším číslom
 - V **druhom** kroku na všetkých smerovačoch nastaviť send-lifetime starého kľúča na uplynulý čas
 - Smerovače postupne prejdú na používanie nového kľúča na odosielanie paketov
 - Prechodný čas, kedy rôzne smerovače používajú rôzny kľúč, nie je problém: prijaté pakety sa overia pomocou toho kľúča, ktorým boli pri odoslaní podpísané
 - Na konci druhého kroku všetky smerovače hladko prešli na používanie nového kľúča a starý zostal nepoužitý
 - V **treťom** kroku starý kľúč z kľúčenky odstránime

Routing Information Protocol v. 2

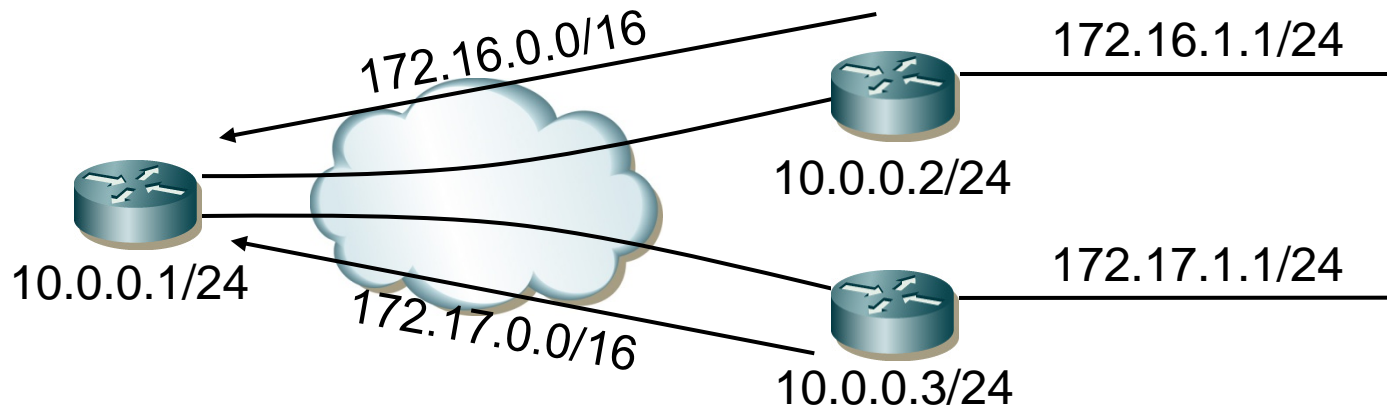
Sumarizácia

- Sumarizácia je popísanie viacerých sietí (komponentov) jedným pokrývajúcim (sumárnym) záznamom
- Pri vhodne navrhnutej adresovej schéme dokáže sumarizácia veľmi efektívne zostručniť výsledné smerovacie tabuľky
- Sumarizácia sa deje **pri odosielaní** smerovacej informácie, nikdy nie pri jej prijatí
- Sumarizácia na Cisco smerovačoch:
 - Automatická (štandardne zapnutá)
 - Manuálna

Routing Information Protocol v. 2

Automatická sumarizácia

- Automatická sumarizácia
 - Ak smerovač posiela informáciu o podsieti istej major network „N“ rozhraním, ktoré leží v inej major network, nahradí túto informáciu záznamom o celej nerozdelenenej sieti „N“
 - Sumarizácia na major network – podľa príslušnej triedy



Routing Information Protocol v. 2

Manuálna sumarizácia

■ Manuálna sumarizácia

- Keď smerovač posiela informáciu o nejakej sieti rozhraním, na ktorom je preddefinovaná sumárna adresa, skontroluje, či táto sieť je podsieťou sumárnej adresy. Ak áno, nahradí informáciu o tejto sieti preddefinovanou sumárnou adresou a maskou.
- Siete, ktoré nie sú podsieťou žiadnej preddefinovanej sumárnej adresy, sa posielajú bezo zmeny
- Ak smerovač neposiela informáciu o nijakom komponente sumárnej adresy, nepošle ani sumárnu adresu

■ Obmedzenia implementácie RIP v Cisco IOS:

- Každá preddefinovaná sumárna adresa musí patriť do inej major network
- Nie je povolený supernetting (agregácia classful sietí)
- Tieto obmedzenia sú obmedzenia IOSu, nie protokolu RIP!
 - <http://nil.uniza.sk/possible-bugslimitations-encountered-ciscos-rip-implementation>

Routing Information Protocol v. 2

Manuálna sumarizácia

- Konfigurácia manuálnej sumarizácie:

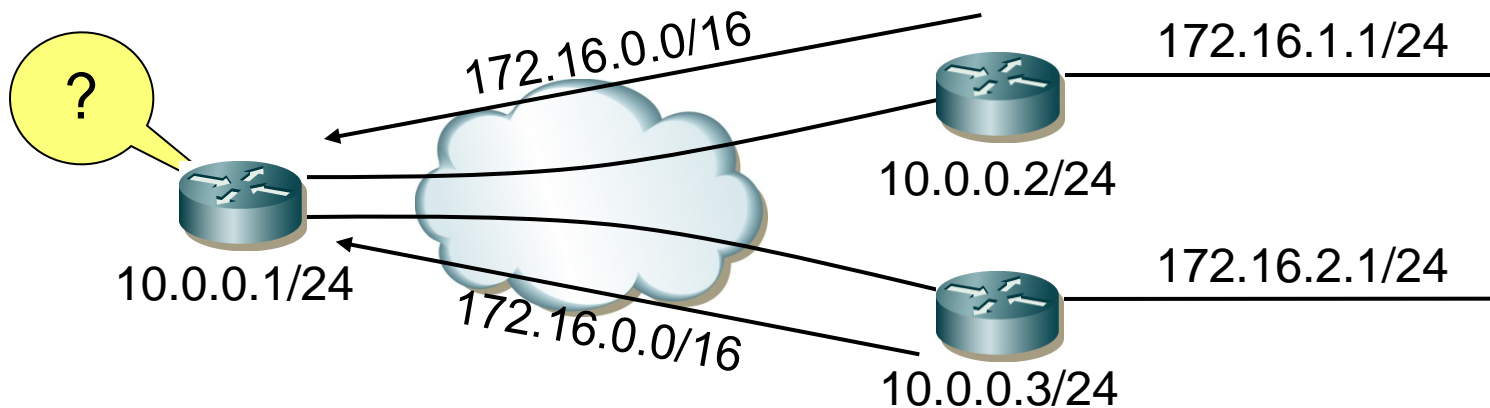
```
Router(config-if)# ip summary-address rip SIET MASKA  
Router(config-if)# router rip  
Router(config-router)# no auto-summary
```

- Automatickú sumarizáciu je potrebné vypnúť, inak bude mať prednosť pred manuálnou sumarizáciou
- Vypnutie automatickej sumarizácie sa odporúča ako samozrejímavý krok pri konfigurácii RIP

Routing Information Protocol v. 2

Network discontinuity

- Nevhodná sumarizácia (v krajnom prípade automatická) spôsobuje problém nazývaný ako network discontinuity
- Network discontinuity:
 - stav, keď podsiete jednej major network sú oddelené medziľahlou sieťou, ktorá leží v inej major network
- Dôsledkom sú nekorektné obsahy smerovacích tabuliek, resp. nekorektné rozhodnutia daného smerovača

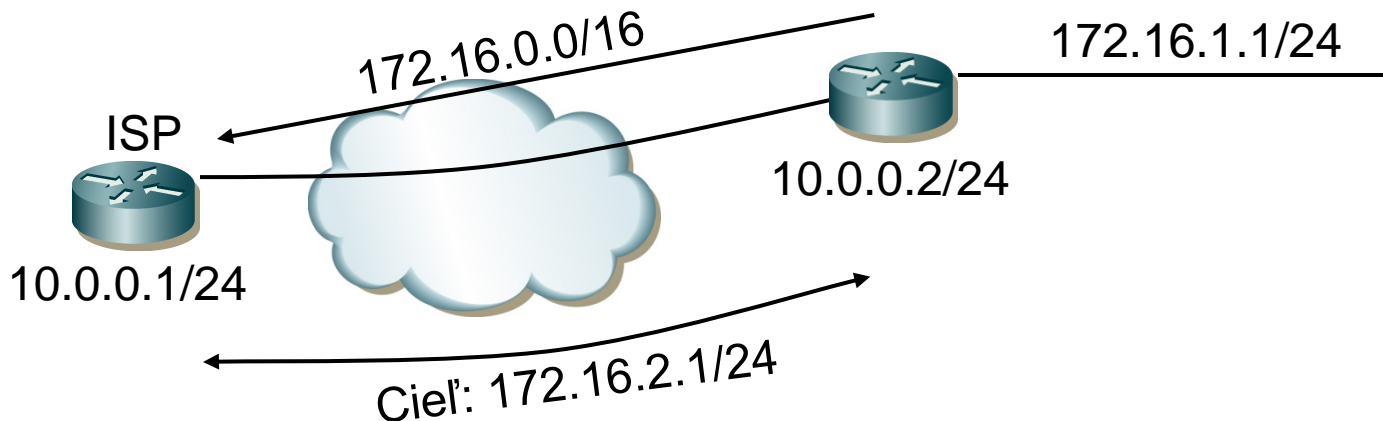


Routing Information Protocol v. 2

Discard route

- Predstavme si situáciu:

- Smerovač posiela k ISP sumarizovanú sieť, ale jeden jej komponent v súčasnosti nie je smerovaču známy
- ISP o tom vďaka sumarizácii nevie a paket určený do neexistujúceho komponentu preposiela nám
- Náš smerovač tento komponent nepozná a paket vráti na ISP vďaka default route – vzniká smerovacia slučka



Routing Information Protocol v. 2

Discard route

- Vznik tejto smerovacej slučky je možné na našom smerovači vyriešiť statickým definovaním tzv. discard route:

```
Router(config)# ip route SIEŤ MASKA Null0
```

kde SIEŤ a MASKA sú identické ako v manuálnej sumárnej položke

- Iné protokoly (EIGRP, OSPF, IS-IS, BGP) si discard route pridávajú automaticky.
- Pri RIP je potrebné pridať ju ručne
 - Ďalšie obmedzenie implementácie RIP v IOSe

Routing Information Protocol v. 2

Konfigurácia pre NBMA siete

- RIPv2 používa multicastovo adresované pakety
 - Dôvod pre multicast/broadcast: dopredu nemusíme vedieť, koľko smerovačov sa na segmente nachádza a aké majú IP
- NBMA siete nie sú schopné prenášať (a rozmnožiť) multicastové rámce
 - Cisco smerovače emulujú tzv. „pseudo-broadcasting“
- Na týchto sieťach je potrebné v RIPv2 vymenovať všetkých priamo pripojených susedov, s ktorými má náš smerovač komunikovať
 - Vymenúvame len tých susedov, s ktorými máme možnosť komunikovať *priamo*,
 - napr. pri hub-and-spoke každý spoke má len jedného suseda – hub router

```
Router(config)# router rip
Router(config-router)# neighbor IP_ADRESA
Router(config-router)# neighbor IP_ADRESA
```

Routing Information Protocol v. 2

Konfigurácia pre NBMA siete

- Teoreticky nie je potrebné vymenovať susedov na point-to-point FR rozhraniach a na multipoint FR rozhraniach, kde IP/DLCI mapovanie má príznak broadcast
 - Nie je nikdy chybou susedov vymenovať
 - „Premature optimization is the root of all evil.“ – D. E. Knuth
- Na multipoint FR rozhraniach je spravidla potrebné vypnúť split-horizon

```
Router(config-if)# no ip split-horizon
```

- Split-horizon pre RIP je štandardne
 - vypnutý na fyzickom FR rozhraní
 - zapnutý na point-to-point a multipoint podrozhraní

Routing Information Protocol v. 2

Konfigurácia pre NBMA siete

- Bug alebo feature: siete zo spoke smerovačov sú z hub routera rozposlané s NH ponechaným na IP adrese spoke routera
 - Pretože medzi spoke smerovačmi nie sú vytvorené PVC, nemôžu sa priamo dosiahnuť, hoci to tak smerovacia tabuľka prikazuje
 - Siete na spoke smerovačoch nedokážu komunikovať, lebo v IP/DLCI map tabuľke bude typicky len IP adresa hub routera
- Riešenie: Na každom spoke smerovači dodefinovať mapovanie medzi IP adresou susedného spoke smerovača a DLCI vedúcim na hub router

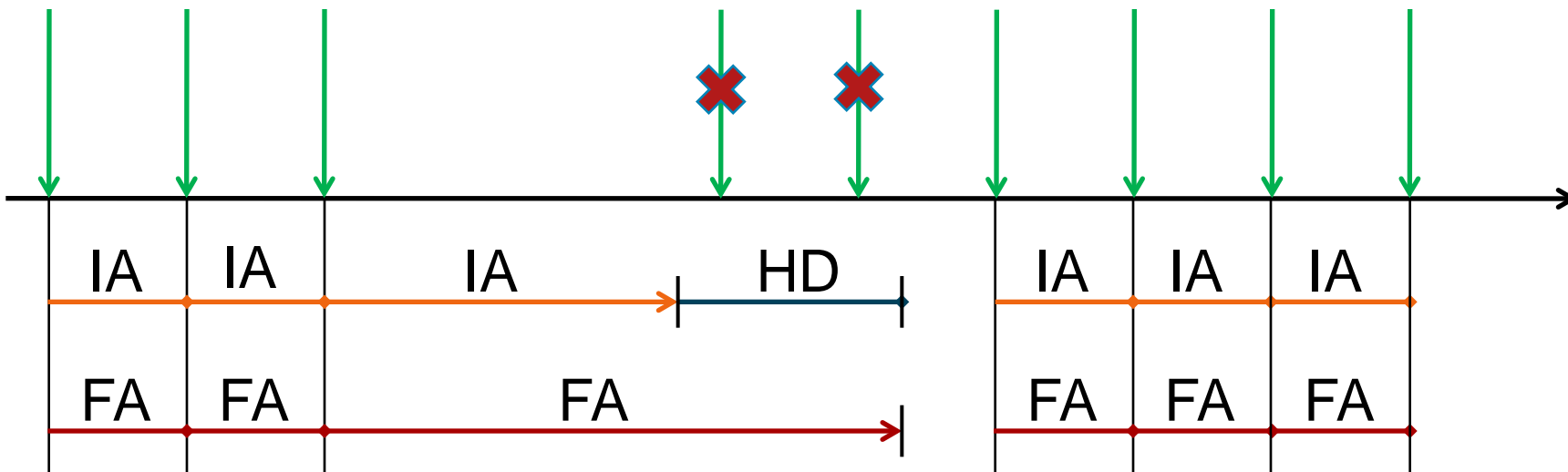
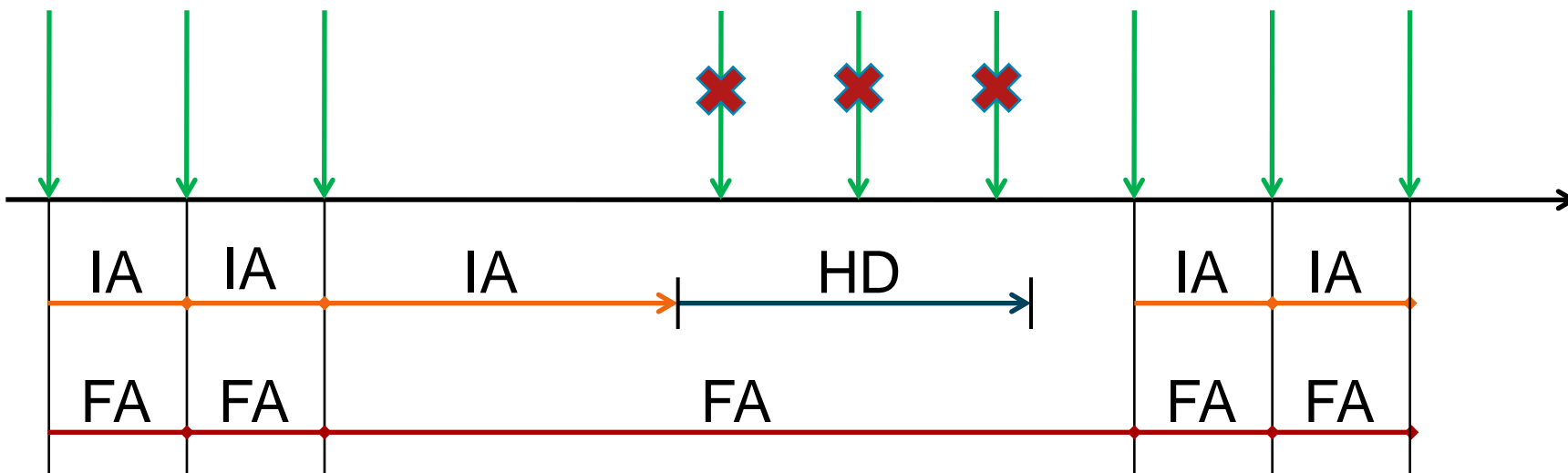
Routing Information Protocol v. 2

Časovače protokolu

- Viaceré aspekty konvergenzie protokolu RIP sú riadené nastaviteľnými časovačmi
- Význam časovačov:
 - **Update**: Interval, v ktorom smerovač posiela do okolia RIP aktualizácie. Štandardne 30 sec.
 - **Invalid after**: Maximálny čas, ktorý môže uplynúť medzi prijatím dvoch za sebou idúcich informácií o istej sieti, než ju prehlásime za neplatnú. Štandardne 180 sec.
 - **Holddown**: Interval, počas ktorého od nikoho neakceptujeme nijakú aktualizáciu o sieti v neplatnom stave. Záznam zostáva v smerovacej tabuľke a používa sa, avšak do okolia sieť ohlasujeme ako nedosiahnuteľnú. Štandardne 180 sec.
 - **Flushed after**: Maximálny čas, ktorý môže uplynúť medzi prijatím dvoch za sebou idúcich informácií o istej sieti, než ju odstránime zo smerovacej tabuľky. Štandardne 240 sec.

Routing Information Protocol v. 2

Časovače protokolu



Routing Information Protocol v. 2

Časovače protokolu

- Pokiaľ sa rozhodneme meniť časovače protokolu, musia byť identicky zmenené na všetkých smerovačoch
- Zmena časovačov:

```
Router(config)# router rip
```

```
Router(config-router)# timers basic UPD INV HOL FLU
```

- Štandardný „Flushed after“ interval je kratší než suma „Invalid + Holddown“

Routing Information Protocol v. 2

Užitečné příkazy

```
show ip protocols
show ip interface
show ip rip database
show ip route A.B.C.D
show key chain
debug ip rip
debug ip routing

ping
ping DEST source SOURCE
```

```
Tclsh

foreach address{
10.0.1.1
10.0.1.129
10.0.2.1
10.0.2.129
10.0.3.1
10.0.3.129
10.0.4.1
10.0.4.129
} {
ping $address
}
```

