
REDES E
COMUNICAÇÕES II

NETWORK DESIGN MODELS

Objectives of Network Design

- Network deve ser **modular** (deve suportar mudanças e evoluções - Scaling the network is eased by adding new modules instead of complete

- Network deve ser **resiliente** onde a rede deve possuir um Uptime perto dos 100\%, uma vez que caso exista uma falha de rede em algumas empresas (ex. financeiro), mesmo por um segundo, pode representar milhões de perdas. E pior ainda nos hospitais, se a uma rede falha, pode pôr em causa vidas.
Obviamente que a resiliência tem um certo custo, visto que o nível de resiliência deve estar entre o *budget* financeiro e o risco.

- Network deve ser **flexível**, pois os negócios tendem a evoluir e a mudar, e, para isso, deve ser possível uma adaptação **rápida** da network.

HIERARCHICAL NETWORK MODEL

◆ Access Layer

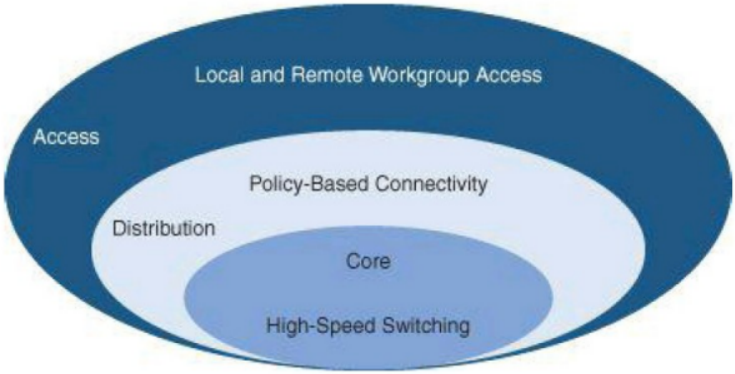
- Providencia um utilizador aceder à network.
- Geralmente incorpora dispositivos switched LAN que permitem conectividade com workstations, IP phones, servidores e pontos de acesso sem fios.
- Para utilizadores remotos ou sites é possível um entrada na network pela tecnologia WAN.

◆ Distribution Layer

- Agrega dispositivos LAN.
- Isola problemas de network.
- Agrega conexões WAN e permite conectividade policy-based

◆ Core Layer

- A high-speed backbone.
- Core is critical for connectivity, must provide a high lever of availability and adapt quickly to changes.
- Should provide stability and fast convergence.
- Should provide an integration point for data center



Network Modules

- Campus
  - Centro de operações de uma empresa
  - Este modelo é onde maior parte dos utilizadores acedem à network
  - Combina uma instrutora CORE de Switching inteligente e uma routing com mobilidade e avançada segurança

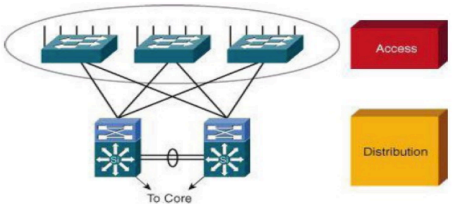
- Data Center
  - Data Centers redundantes providenciam um backup e replicação de aplicação
  - Network e os dispositivos oferecem ao servidor e aplicativos load balanceamento to maximizar a performance

- Permite à empresa escala sem muitas mudanças na infrastutura
- Branch
  - Permite a empresas extender aplicações head-office e serviços para localizações remotas e utilizadores ou pequenos grupos de branches.
  - Permite à empresa um cost-effectively presence em largas áreas geográficas
  - Segurança é providenciada com múltiplos serviços VPN de comunicação sobre Layer 2 ou 3

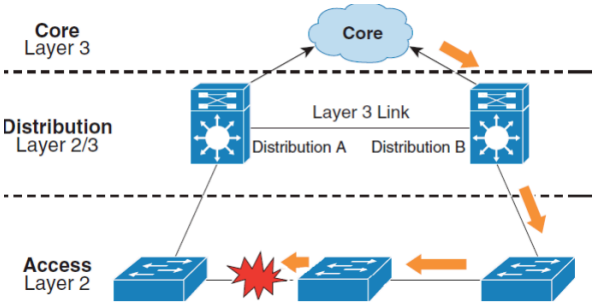
- WAN and MAN
  - Oferece uma convergência de áudio, vídeo e serviços de data
  - Providencia segurança a voz, mission-critical data, and video applications
  - Deve providenciar uma arquitetura robusta com altos níveis de resiliência para todos os branch offices.

- Remote User
  - Permite a empresas entregar áudio e data em segurança para um pequeno office/home office remotos (SOHO) sobre uma standard broadband access service
  - Permite uma entrada na network sobre uma VPN e acesso a serviços e aplicações autorizadas

Designing the Access Layer



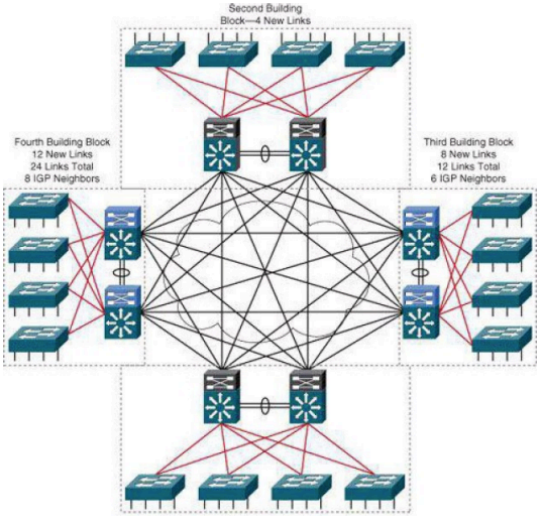
Alta disponibilidade - Default gateway redundancy using multiple connections from access switches to redundant distribution layer switches & Redundant power supplies



Daisy Chain is a wiring scheme in which multiple devices are wired together in sequence or in a ring, similar to a garland of daisy flowers.

- When using a L2 link between Distribution layer switches:
  - Daisy Chain é aceitável, no entanto pode sobrecarregar algumas Access layer switches e ainda pode aumentar a convergência de STP em caso da falhas

Without a Core Layer

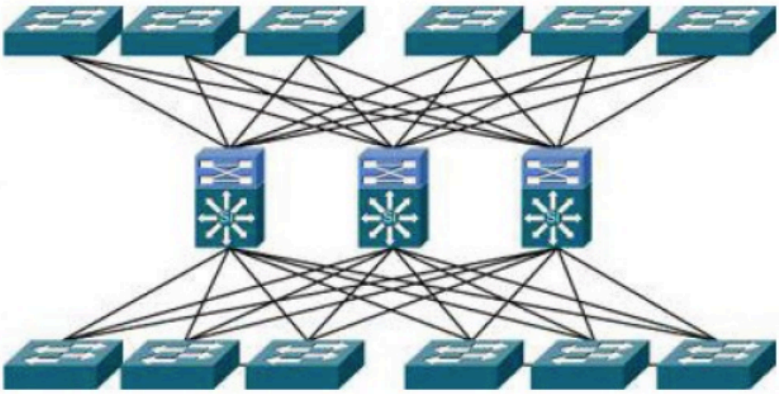


Observando a figura acima:

- Pode ser **difícil** de escalar e compreender
- **Aumenta** a necessidade de cabos
- **Complexidade** dos routers num design full-mesh aumenta assim que os Neighbours são adicionados
- Pode ser usado em **pequenos** campos **sem perspetiva de crescimento**

Em pequenas networks, o Core e distribution layer pode ser só uma eliminando a necessidade de hardware de switching extra e simplifica a implementação da network. No entanto, elimina as vantagens de ter uma arquitetura de múltiplas layers, especialmente *fault isolation - identifies when a fault has occurred, and pinpointing the type of fault and its location.*

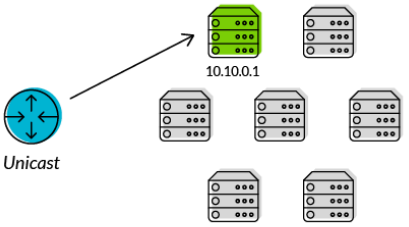
Avoid Too Much Redundancy

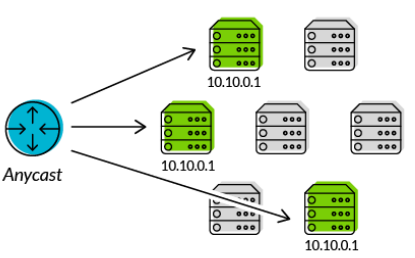


Demasiada redundância aumenta:

- *Complexidade de routing*
- *Número de portas usadas*
- *Wiring*

IP UNICAST ROUTING





IP Routing Overview

- Routers encaminham pacotes para redes de destino

- Routers devem conhecer as networks destino para encaminhar os pacotes

- O router conhece as networks que estão diretamente conectadas com as suas interfaces

- Para networks não diretamente conectadas com as suas interfaces o router deve depender de informação vizinha

- O router pode conhecer as networks remotas a partir de:

  ➡ **Static Routing** - Um administrador configura manualmente a informação

  ➡ **Dynamic Routing** - Aprende com os outros routers

  ➡ **Policy Based Routing** - Excedem Static/ Dynamic Routing e podem depender de parÂmetros para além do endereço destino

Default Routes

- Em algumas circunstâncias, um router não precisa de reconhecer os detalhes de networks remotas

- O router pode ser configurado para mandar todo o tráfico (ou todo o tráfico pela qual não há uma entrada mais específica routing table) para um específico neighbour router

- É conhecido Default Route

- Default Routes são dinamicamente anunciados usando protocolos de routing ou então são estaticamente configurados.

- IPV4 default route - 0.0.0..0/0

- IPV6 default route - ::/0

Static Routing,, Não Mexe

Static Routing Examples

- Static routing não reage a mudanças na network
- Static Routing não altera quando a network cresce
- Static Routing é usado quando :
  - o administrador necessita controlo total sobre todas as rotas usadas pelo router
  - o backup para uma rota dinamicamente reconhecida é necessária
  - é usada para alcançar uma network acessível por um único path (não existe backup link, por isso dynamic routing não apresenta vantagens)
  - o router conecta-se ao seu ISP e precisa de apenas uma rota default apontada para o router ISP, em vez de aprender várias rotas pelo ISP
  - o router é insuficientemente potente e não tem CPU ou recursos de memória necessários para aguentar um protocolo de dynamic routing.
  - não é desejado ter dynamic routing updates forwarded across baixa banda larga

Dynamic Routing

- Dynamic routing permit que a network se ajuste a mudanças automaticamente sem precisar do envolvimento do admin

- Routers trocam informação sobre networks atingíveis e o estado de cada network/link
    - Routers exchange information only with other routers running the same routing protocol
    - When the network topology changes, the new information is dynamically propagated throughout the network, and each router updates its routing table to reflect the changes

Administrative Distance

- O protocolo/método com a **menor** Administrative Distance é preferida

- Dentro do **mesmo Autonomous System (AS), a Administrative Distance = 200**, caso haja comunicação entre dois routers que pertençam a **diferentes AS's Administrative Distance = 20**

- Exemplo
    - Static [**1**/1] 192.168.1.0/24 via ... ← Chosen!
    - RIP [**120**/1] 192.168.1.0/24 via ...
    - OSPF [**110**/1] 192.168.1.0/24 via ...

Autonomous Systems

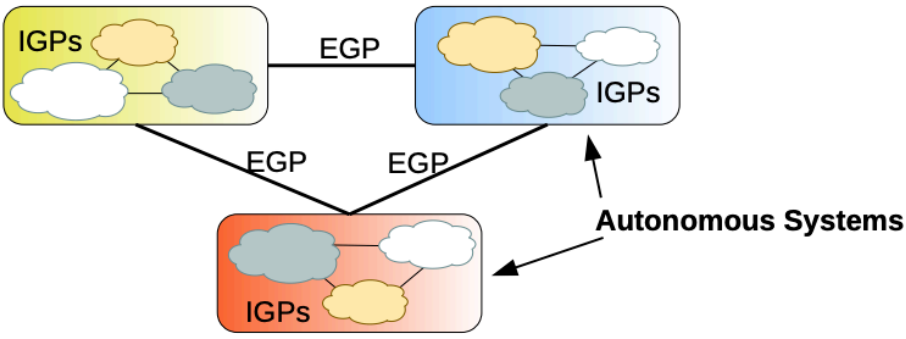
AS (Autonomous System) – set of routers/networks with a common routing policy and under the same administration.

- Routing **inside** an AS is performed by **IGPs** (Interior Gateway Protocols) such as **RIPv1**, RIPv2, **OSPF**, IS-IS and EIGRP

- Routing **between** AS is performed by **EGPs** (Exterior Gateway Protocols) such as **BGP**

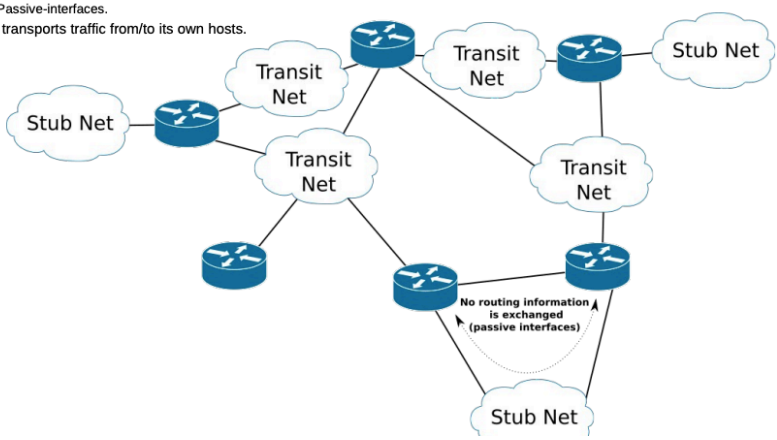
- IGPs: optimize routing performance

- EGPs: optimize routing performance obeying political, economic and security policies



Type of Networks

- Transit/Transport
  - Used to interconnect networks.
    - Routers exchange routing information using it.
  - Transports traffic from/to other network hosts and from/to its own hosts.
- Stub
  - Single router network.
  - or multiple routers network, if routers do not exchange routing information.
    - Passive-interfaces.
  - Only transports traffic from/to its own hosts.



Distance Vector Vs Link State Protocols

Distance Vector

- Os routers aprendem a rede através da informação enviada pelos routers vizinhos, com essa informação e usando uma versão assíncrona do Bellman-Ford algorithm calculam os seus custos. Exemplos: RIPv1, RIPv2, IGRP, EIGRP.

Link State

- Os routers aprendem toda a rede usando um algoritmo centralizado para calcular o caminho mais perto para todas as redes conhecidas. A informação é passada através de flooding, os routers com essa informação constroem as suas tabelas. Exemplos: OSPF, IS-IS.

Distributed and Asynchronous Bellman-Ford Algorithm

- Cada node periodicamente envia para os seus vizinhos o seu custo até ao destination node.

- Cada node recalcula o seu próprio custo e envia a atualização.

RIP (Routing Information Protocol)

É um distance vector protocol, cada router mantém uma lista das redes que conhece e o custo para chegar até elas (Distance Vector), cada router anuncia periodicamente o seu próprio custo (parcial ou completo) (announcement/update). Cada router usa os valores enviados pelos seus vizinhos para atualizar o seu custo.

RIP Version 1

RIPv1 é um protocolo que **não** anuncia **máscaras** (netmask) de rede, por isso usa a mascara da interface que recebeu o pacote, para usar este protocolo todas as redes têm de ter a mesma mascara. Usa o endereço de **broadcast 255.255.255.255** para enviar updates e não suporta autenticação o que o torna vulnerável a ataques maliciosos.

RIP Version 2

RIPv2 adiciona ao RIPv1 a **capacidade de suportar diferentes máscaras** (netmasks). O endereço de **broadcast para updates é diferente - 224.0.0.9**, estes pacotes são **apenas** enviados para routers a correr o RIPv2.

Count to Infinity Problem

Quando acontecem falhas antes de o algoritmo estabilizar criam-se os pacotes **infinitos** que enquanto não chegam ao seu destino continuam **sempre** a ser passados **infinitamente**.

Split-Horizon

Para combater o problema do Count to Infinity, recorre-se ao **split horizon,** onde cada router, em cada interface anuncia apenas as networks que não são usadas para chegar ao destino (root)

RIP Message Types

- **RIP Response**
  - Contém Distance vector
  - É enviado:
    1. Periodicamente (default são ~30seg, existe uma componente random)
    2. Opcionalmente, quando alguma informação muda
    3. Em resposta ao RIP Request

- **RIP Request (Optional)**
  - Enviado pelo o router que foi recentemente iniciado (bootstrap) ou quando a validade de alguma da informação do distance vector tenha expirado (default timeout = 180 s)

RIPv1 vs RIPv2 Responses

Os pacotes do RIPv2 possuem alguns campos a mais em relação ao RIPv1:

- Subnet Mask, suporta tamanhos de masks variáveis e passa a **mascara da rede** e faz o RIPv2 ser um **classless** protocol.

- Route tag, usado para separar redes internas (to the RIP domain) e externas.

- Next Hop,, endereço para os quais os pacotes devem ser routed, 0.0.0.0 indica que o pacote deve ser enviado para o router que enviou o pacote (RIP message).

RIPng for IPv6 Routing

Similar com o IPV4 RIPv2, em vez de IPV4 como transporte utiliza IPV6

Permite custos para alem de 1,, infinity metric value = 16

RIPng Path Costs

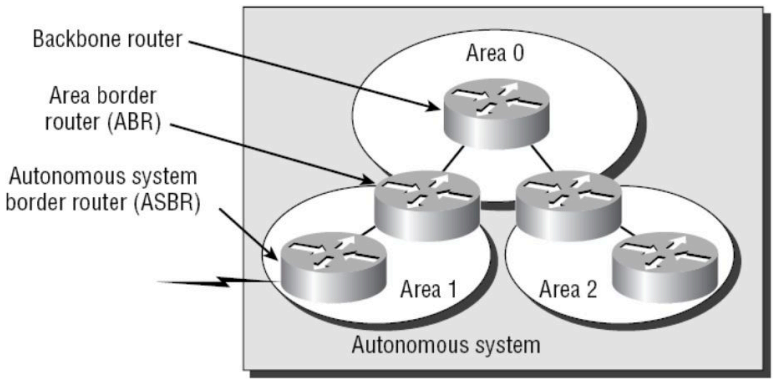
Os custos são a soma de todos os custos até á rede em questão.

Open Shortest Path First (OSPF) Protocol

- **OSPF** é um protocolo de routing **link-state**, pelo que responde **rápido a mudanças** na network, envia **updates** quando ocorre mudanças e ainda envia updates periodicamente, conhecidos como link-state refresh, entre 30 minutos de **intervalo**

- Routers que correm OSPF recolhem informação routing de todos os outros routers na network (ou dos de uma área de network definida)

- Cada router independentemente calcula os melhores caminhos para todos os destinos da network através do algoritmo de Dijkstra's (SPF)



OSPF Necessary Routing Information

Para que todos os routers da network façam decisões de routing consistentes, cada router link-state deve guardar a seguinte informação:

- **Neighbour Routers**
  - Caso um router perca contacto com o router vizinho, em poucos segundos invalida todos os caminhos que passem por esse router e recalcula os caminhos pela network

- O router reconhece os outros routers e networks através de **LSA's** (LINK STATE ADVERTISEMENTS), que são *flooded* pela network

- Melhores caminhos para cada destino:
  - Cada router independentemente calcula os melhores caminhos para todos os destinos da network através do algoritmo de Dijkstra's (SPF)
  - Todos os pacotes são guardados na LSDB (Link State Data Base)
  - Os melhores caminhos são oferecidos À routing table
  - Pacotes vindos até ao router são enviados com a informação que contém a routing table

OSPF Packets

- **Hello -** Descobre vizinhos e constrói adjacencies entre eles.

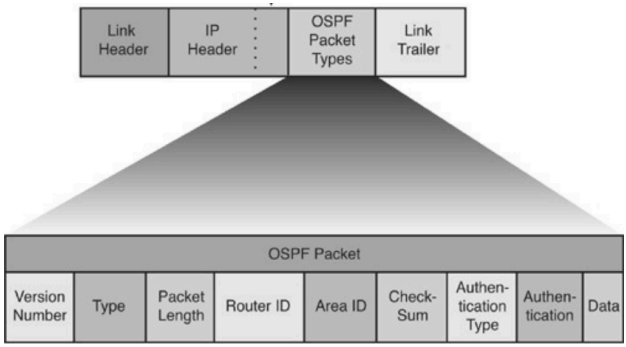
- **Database Description (DBD) -** Confirma sincronização de database entre os routers

- **Link-State Request (LSR) -** Pede certos link-state records de outro router

- **Link-State Update (LSU) -** Envia especificamente

- **LSAck -** Reconhece os outros tipos de pacotes requested link-state records

OSPF Packet Format



OSPF Areas

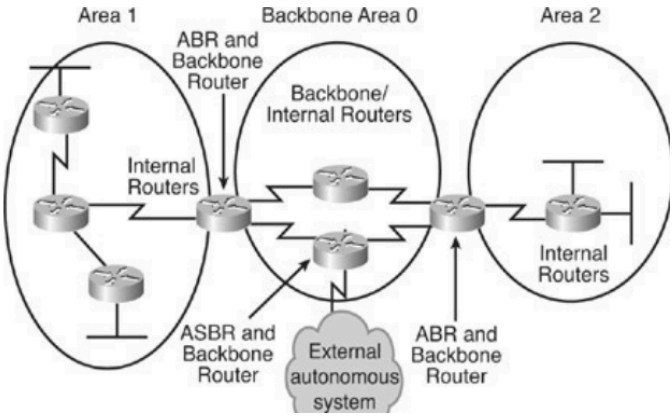
Vantagens:

- Reduzida frequência do cálculo de SPF (Shortest Path First) - sós os routers afetados com mudanças na network precisam de recalcular o SPF algorithm e o impacto da mudança localiza-se dentro da área a que estes pertencem.

- Menos updates overhead

- Routing Tables mais pequenas

OSPF Routers Types



View while making this masterpiece

ABOUT THE AUTHOR

João Afonso Pereira Ferreira (103037) - MIECT - Mestrado Integrado de Engenharia de Computadores e Telemática. Com recurso aos slides fornecidos pelo docente Paulo Salvador.