Arquitetura de Comunicações - Resumo para Exame

1. Quality of Service (QoS)

1.1 Conceitos Fundamentais

Necessidade de QoS:

- Redes multiservices com requisitos heterogéneos
- Diferentes aplicações têm diferentes necessidades:
    - **Packet loss**: algumas aplicações (áudio/vídeo) suportam perdas; outras (FTP, telnet) requerem 100% de sucesso
    - **Bandwidth**: aplicações multimedia requerem largura de banda mínima; aplicações elásticas (email, FTP) usam o que está disponível
    - **Timing (delay e jitter)**: telefonia e jogos requerem baixos atrasos; outras aplicações não têm limites estritos

Tipos de Aplicações:

- **Elásticas**: usam qualquer largura de banda disponível (FTP, email)
- **Inelásticas**: necessitam de largura de banda mínima (multimedia)
    - Adaptativas: funcionam com BW inferior ao nominal
    - Rígidas: não funcionam com BW inferior ao nominal

1.2 Princípios de Garantia de QoS

Princípio 1 - Packet Marking:

- Necessário marcar pacotes para o router distinguir entre tipos de tráfego
- Permite aplicar políticas diferentes no router

Princípio 2 - Policing:

- Forçar conformidade das fontes com a largura de banda acordada
- Marcação e policing na entrada da rede
- Proteção (isolamento) de uma classe de tráfego em relação a outra

Princípio 3 - Uso Eficiente:

- Usar recursos de forma eficiente
- Evitar atribuição fixa de BW que pode não ser utilizada

Princípio 4 - Call Admission:

- Fluxo declara requisitos
- Rede pode bloquear a chamada se não conseguir suportar

1.3 Traffic Conditioning

Leaky Bucket:

- Parâmetros: p (tamanho do bucket), b (taxa de saída)
- Dados entram a qualquer taxa, saem a taxa constante
- p/b é o atraso máximo na transmissão
- Limita bit rate à taxa b

Token Bucket:

- Parâmetros: b (tamanho do bucket), r (taxa de tokens), p (taxa de pico)
- Bucket enche com tokens à taxa r
- Transmissão possível se há tokens
- Permite bursts com taxa p
- Total de dados enviados em tempo t < rt + b
- Taxa média nunca excede r

1.4 Técnicas de Gestão de Filas

Tail Drop:

- Pacotes são descartados quando buffer está cheio
- Problema: sincronização global de fontes TCP

RED (Random Early Detection):

- Lida com congestão antes de aparecer
- Probabilidade de perda de pacote proporcional ao comprimento da fila
- Parâmetros: minQ, maxQ, maxP
- Reduz sincronização global do TCP

WRED (Weighted RED):

- 3 níveis de descarte para diferentes prioridades
- Últimos a ser descartados são os de maior prioridade

1.5 Algoritmos de Scheduling

FIFO:

- Não faz diferenciação de QoS
- Fluxos com n vezes mais tráfego recebem n vezes mais serviço

Priority Queuing:

- Classificação por prioridade
- Tráfego de prioridade alta sempre servido primeiro
- Fluxos de alta prioridade podem impedir serviço aos de baixa

Fair Queuing (FQ):

- Largura de banda distribuída igualmente entre filas não vazias
- 33.3% para cada fila (se 3 filas)

Weighted Fair Queuing (WFQ):

- Cada fila recebe percentagem da largura de banda igual ao seu peso dividido pela soma dos pesos

- Exemplo: pesos 2, 3, 4 → 2/9, 3/9, 4/9 da largura de banda

2. Integrated Services (IntServ)

2.1 Tipos de Serviço

Controlled Load (CL) - RFC2211:

- Serviço E2E independente da carga
- Pacotes recebidos com atrasos mínimos nos routers

Guaranteed Service (GS) - RFC2212:

- Garante serviço E2E em termos de delay para uma dada largura de banda
- D = b/R (delay máximo)

Best Effort (BE):

- Não garante qualidade de serviço, apenas existência de conexão

2.2 RSVP (Resource Reservation Protocol)

Características:

- RFC 2205
- Encapsulado em IP (protocolo tipo 46)
- Baseado em troca de mensagens PATH e RESV

Operação:

1. **PATH**: anuncia características de tráfego do emissor
2. **RESV**: confirma reservas, iniciado pelos receptores
3. Estados dos routers devem ser refrescados periodicamente (soft states)

Parâmetros Genéricos:

- NON_IS_HOP: nó não suporta IntServ
- NUMBER_OF_IS_HOPS: contador de nós QoS-aware
- AVAILABLE_PATH_BANDWIDTH: largura de banda disponível
- MINIMUM_PATH_LATENCY: atraso do caminho
- TOKEN_BUCKET_TSPEC: especificações de tráfego (r, b, p, m, M)

Estilos de Reserva:

- **Fixed Filter**: recetor especifica valor de reserva por cada emissor
- **Wildcard Filter**: recetor define valor único para receber de qualquer emissor
- **Explicit Filter**: recetor especifica lista de emissores e valor único

2.3 Problemas do IntServ

- **Não escala no core**: baseado em fluxos individuais
- Requer estado por fluxo em cada router
- Complexidade aumenta com número de fluxos

3. Differentiated Services (DiffServ)

3.1 Objetivos

- Escalabilidade para o core da rede
- Sem estado por fluxo
- Sem sinalização por fluxo
- Simples de implementar no core
- Controlo de agregados de tráfego

3.2 Arquitetura

Componentes:

1. **PHB (Per-Hop-Behavior)**: tratamento de pacotes nos routers
2. **Traffic Control**: fundamentalmente nas bordas
3. **Separação de serviços**: independente de restrições técnicas da rede

Field DS (DSCP - 6 bits):

- Marcado no campo TOS (IPv4) ou Traffic Class (IPv6)
- Define a classe de serviço do pacote

3.3 Classes de Serviço

Default (DE) - DSCP = 000000:

- Serviço best-effort com fila única FIFO

Expedited Forwarding (EF) - DSCP = 101110:

- Serviço "Virtual Leased Line"
- Controlo de perdas, delay e jitter
- Baixo delay, pequeno jitter, sem perdas
- Policing rigoroso na borda

Assured Forwarding (AF) - DSCP = aaadd0:

- QoS relativa (AFi servido com mais BW que AFj para i<j)
- 4 classes, 3 níveis de precedência de descarte em cada
- Pacotes dentro do perfil não são geralmente perdidos
- Pacotes fora do perfil podem ser tratados como BE

3.4 Border (Edge) Routers

Funções:

- **Meters**: verificam características temporais do fluxo vs SLA
- **Classifiers**: identificam classe de tráfego do pacote
- **Markers**: definem DSCP para cada pacote (in/out profile)
- **Droppers**: removem pacotes fora de perfil
- **Shapers**: atrasam pacotes fora de perfil usando buffers

3.5 Problemas do DiffServ

- Sem standards para SLAs
- Mesmo DSCP pode ser usado por serviços diferentes entre ISPs
- Falta de simetria (TCP funciona melhor em ambientes simétricos)
- Sem suporte para multicast

4. Content Distribution Networks (CDN)

4.1 Motivação

Problemas a Resolver:

- Flash crowds (exemplo: 11 de Setembro)
- Congestão de rede
- Carga excessiva em servidores
- Latência elevada

Soluções Inadequadas:

- **Server Farms**: não resolvem problemas de congestão de rede
- **Caching Proxies**: servem apenas clientes locais, sem controlo do content provider

4.2 Conceitos

CDN:

- Rede de servidores que entrega conteúdo em nome de um site origem
- Sem software customizado no cliente
- Sem software customizado no servidor
- Sem pré-posicionamento

Características:

- Edge servers em múltiplas localizações ISP
- Evita porções congestionadas da Internet
- Melhora tempo de resposta
- Offload de objetos intensivos em largura de banda

4.3 Gerações de CDN

1ª Geração (anos 90):

- Static caching
- Acelerar performance de websites

2ª Geração (anos 2000):

- Dynamic content
- Suporte a tráfego multimedia elevado

3ª Geração (2010s):

- Cloud integration, SDN CDNs

- UGC (user generated content)
- Suporte mobile

4ª Geração (2020+):

- Edge e federação
- Integração com ambientes mobile
- Edge devices (MEC)
- Federação multi-operador

4.4 Componentes

Distribution Infrastructure:

- Mover/replicar conteúdo de origem para surrogates

Request Routing Infrastructure:

- Direcionar pedidos de clientes para surrogate adequado
- DNS-based redirection (mais comum)

Accounting Infrastructure:

- Logging e reporting de atividades

4.5 DNS Redirection

Vantagens:

- Usa infraestrutura DNS escalável existente
- URLs podem permanecer iguais

Limitações:

- Servidores DNS veem apenas IP do DNS server
- Content owner deve ceder controlo
- Endereços unicast podem limitar reliability

5. Network Management

5.1 Áreas de Gestão (ISO - FCAPS)

Fault Management:

- Deteção, isolamento e correção de comportamentos anómalos
- Manter logs de erros
- Criar notificações de erros
- Realizar testes de diagnóstico

Configuration Management:

- Controlo de dados para elementos de rede
- Definir parâmetros que controlam operação do sistema
- Modificar configuração do sistema

Accounting Management:

- Medir utilização da rede
- Determinar custos e accountings de utilizadores
- Controlo de acesso por utilizador

Performance Management:

- Avaliar/reportar comportamento/eficiência de equipamentos
- Obter informação estatística
- Manter logs de estado do sistema

Security Management:

- Suportar gestão segura de comunicações
- Controlo de serviços e mecanismos de segurança
- Reportar eventos associados a segurança

5.2 Modelos de Gestão

Centralizados:

- Modelo agente-manager
- Manager contém inteligência para decisões
- Agente opera com equipamento e reporta ao manager

Distribuídos:

- Partilha de responsabilidades de gestão

Hierárquicos:

- Estrutura hierárquica com informação centralizada na raiz

5.3 SNMP (Simple Network Management Protocol)

Estrutura:

- Manager: aplicação de gestão
- Agent: software nos equipamentos geridos
- MIB (Management Information Base): base de dados de objetos geridos
- Protocolo de gestão (SNMP PDUs sobre UDP)

Tipos de Mensagens:

- **GetRequest, GetNextRequest, GetBulkRequest**: Manager → Agent (obter dados)
- **SetRequest**: Manager → Agent (definir valor MIB)
- **Response**: Agent → Manager (resposta a Request)
- **Trap**: Agent → Manager (notificação de exceção)
- **InformRequest**: Agent → Manager (informação confiável)

Operação:

- **Polling**: Manager pergunta periodicamente ao agent
    - Vantagem: controlo completo

        - Desvantagem: delay entre evento e entrada no sistema; overhead
- **Traps**: Agent envia quando ocorre evento
    - Vantagem: informação apenas quando necessário
    - Desvantagem: mais recursos no equipamento gerido

OSI Object Identifier Tree:

- Nomenclatura hierárquica para objetos
- Cada nó tem nome e número
- Exemplo: 1.3.6.1.2.1.7.1 (udpInDatagrams)

ASN.1 e TLV Encoding:

- ASN.1: linguagem formal para descrever SMI
- BER (Basic Encoding Rules): formato de transmissão
- TLV: Type, Length, Value encoding

RMON (Remote Monitoring):

- RFC 1757 (RMON1), RFC 2021 (RMON2)
- Probes para análise de rede (modo promíscuo)
- 9 grupos: Statistics, History, Alarm, Host, HostTopN, Matrix, Filter, Packet Capture, Event

Prós e Contras:

- **Prós**: amplamente usado, simples, robusto, extensível
- **Contras**: não escala, overhead de comunicação, semântica específica dificulta integração

5.4 Policy Based Management (PBM) - COPS

Conceito:

- Gerir globalmente a rede, não os seus elementos
- Definir políticas (regras) para informar a rede do que fazer

Elementos:

- **Policy Management Tools**: criar regras de política
- **Policy Repository**: armazenar regras
- **Policy Decision Points (PDP)**: tomar decisões e transferir regras
- **Policy Enforcement Points (PEP)**: elementos afetados pelas regras

COPS (Common Open Policy Service):

- Protocolo pergunta/resposta para interação PDP-PEP
- Baseado em TCP
- Mantém sincronização de estado
- Dois tipos de clientes:
    - **Outsourcing (RSVP)**: PEP contacta PDP quando decisão é necessária
    - **Configuration (DiffServ)**: PDP configura PEP com informação específica

Operação COPS:

1. PEP abre sessão COPS (especificando tipo de cliente)
2. PEP envia pedidos e recebe respostas

3. PDP pode mudar comandos previamente enviados
4. PEP envia mensagens sobre utilização de recursos
5. KeepAlives enviados se não há atividade

5.5 CMIS/CMIP (OSI Management)

Common Management Information Protocol:

- Desenhado nos anos 80 como protocolo unificador
- Implementação lenta comparada com SNMP

Características:

- Abordagem orientada a objetos
- Objetos têm atributos, geram eventos, executam operações
- Classes de objetos
- Agentes inteligentes (podem usar regras/políticas)
- Ações: GET, SET, CREATE, DELETE, ACTION, NOTIFICATION, CANCEL_GET

GDMOs (Guideline for Definition of Managed Objects):

- Modelam objetos dentro do equipamento
- Instanciação de GDMOs é chamada MIB
- Grande liberdade de implementação (flexibilidade e complexidade)

Arquitetura:

- CMISE: acesso remoto e manipulação de objetos
- ROSE: operações e notificações remotas
- ACSE: estabelecimento, gestão e terminação de associações

Prós e Contras:

- **Prós**: orientado a objetos, flexível, suporte da indústria telecom, interação manager-manager
- **Contras**: complexo, multi-camada, grande overhead, poucos sistemas baseados em CMIP

Comparação SNMP vs CMIS:

- SNMP: MIBs estáticas, não orientado a conexão, polling, ligth, domina mercado
- CMIS: MIBs dinâmicas, orientado a conexão, event-oriented, heavy, relevância em telecom

5.6 TMN (Telecommunications Management Network)

Objetivo:

- Suportar gestão de redes e serviços de telecomunicações
- Estrutura organizada para interconexão de sistemas operativos e equipamentos telecom

Modelo Multi-Camada:

1. **Network Element Layer (NEL)**: deteção de falhas, geração de traps
2. **Element Management Layer (EML)**: gestão de alarmes, backup, logging
3. **Network Management Layer (NML)**: configuração, controlo, supervisão da rede
4. **Service Management Layer (SML)**: handling de serviços, políticas, SLAs
5. **Business Management Layer (BML)**: contacto com clientes, análise de tendências, billing

Arquitetura Física:

- **Operation System (OS)**: funcionalidade principal de gestão
- **Mediation Equipment (MD)**: mediação entre OS e NE
- **Network Element (NE)**: equipamentos geridos
- **Workstation (WS)**: acesso de utilizador
- **Data Communication Network (DCN)**: onde flui informação de gestão
- **Adapter Q (QA)**: adaptação de equipamentos não-TMN

Interfaces Standard:

- **Q3**: Operation System ↔ elementos TMN (normalmente CMIP)
- **Qx**: Mediation Element ↔ Network element/adapter
- **F**: Workstation ↔ Operation system/mediator
- **X**: TMN ↔ TMN ou rede com interface TMN

TMN Matrix:

- Funcionalidade FCAPS ao longo das camadas TMN

Relação com OSI:

- TMN adiciona à gestão OSI
- Modelo de informação de rede
- Modelo de organização através de blocos funcionais
- Modelo de comunicação (correspondência interface-protocolo)
- Modelo funcional com novas funções de gestão de rede

6. BGP (Border Gateway Protocol)

6.1 Conceitos Fundamentais

BGP:

- Versão 4 (BGP4) implementada em 1993
- Protocolo que assegura conectividade da Internet
- Usado principalmente para routing entre Autonomous Systems (AS)

Autonomous System (AS):

- Rede sob uma única administração
- Operador(es) de rede com política de routing global bem definida
- AS Number: ID alocado pela InterNIC, globalmente único
- RFC 4271: AS number de 2 bytes (1-64511 público, 64512-65535 privado)
- RFC 4893: suporte para AS numbers de 4 bytes

Tipos de BGP:

- **eBGP (External BGP)**: entre ASs diferentes
- **iBGP (Internal BGP)**: dentro do mesmo AS
    - Routers iBGP devem manter sessão com todos os outros iBGP routers (iBGP Mesh)
    - Exceção: route reflectors

6.2 Relações de Vizinhança

Peering:

- Geralmente configurado manualmente
- Cada sessão corre sobre TCP (porta 179)
- Peers trocam todas as rotas quando sessão é estabelecida
- Updates enviados quando há mudança na topologia ou política
- KEEPALIVE messages para evitar inatividade

ASBR (Autonomous System Border Router):

- Routers que implementam relações de vizinhança BGP

6.3 Tipos de AS

Single-homed (Stub) AS:

- AS com apenas um border router
- Único acesso Internet
- Único ISP

Multi-homed Non-transit AS:

- AS com mais de um border router
- Múltiplos acessos Internet
- Múltiplos ISPs
- Não transporta tráfego de outros AS

Multi-homed Transit AS:

- AS com mais de um border router
- Múltiplos acessos Internet
- Transporta tráfego de outros AS

6.4 Path-Vector Protocol

Características:

- Protocolo distance-vector que transporta lista de AS atravessados pela rota
- Deteção de loops
- eBGP speaker adiciona seu AS à lista antes de encaminhar
- iBGP speaker não modifica a lista (mesmo AS)

6.5 Mensagens BGP

OPEN:

- Estabelece sessão BGP
- Negocia capacidades

UPDATE:

- Envia prefixos de routing com atributos BGP associados
- Contém:

    - Withdrawn routes: redes IP não mais acessíveis
    - Path attributes: parâmetros para definir routing e políticas
    - NLRI: redes IP com conectividade

KEEPALIVE:

- Trocado quando período keepalive é excedido sem update

NOTIFICATION:

- Enviado quando erro de protocolo é detetado
- Sessão BGP é fechada após

6.6 Atributos BGP

Categorias:

1. **Well-known Mandatory** (incluídos em updates BGP):
    - AS-PATH, Next-Hop, Origin
2. **Well-known Discretionary** (podem ou não ser incluídos):
    - Local Preference, Atomic Aggregate
3. **Optional Transitive** (podem não ser suportados):
    - Aggregator, Community, AS4_Aggregator, AS4_Path
4. **Optional Non-transitive**:
    - Multi-Exit Discriminator (MED)
5. **Cisco-defined** (local ao router):
    - Weight

Atributos Principais:

AS-PATH:

- Lista ordenada de AS atravessados pela rota
- Usado para deteção de loops

ORIGIN:

- Indica como BGP aprendeu a rota
- IGP (0): rota interior ao AS originador
- EGP (1): não mais usado
- INCOMPLETE (2): aprendida por outros meios (redistribuição)

Next-Hop:

- Endereço IP usado para alcançar o router que anuncia
- Para eBGP: IP da conexão entre peers
- Para iBGP: endereço next-hop eBGP é propagado no AS local
    - Pode ser configurado como border router com next-hop-self

Local Preference:

- Usado para escolher ponto de saída do AS local
- Valor maior é preferido
- Propagado através do AS local

- Pode ser diferente para rotas diferentes

MED (Multi-Exit Discriminator):

- Sugestão para AS externo
- Valor menor é preferido
- Desenhado para influenciar tráfego de entrada

Weight (Cisco):

- Atributo local ao router
- Não anunciado a vizinhos
- Valor maior é preferido

Atomic Aggregate:

- Alerta que rotas específicas foram agregadas numa menos específica
- Rotas mais específicas são perdidas

Aggregator:

- Informação sobre qual AS fez agregação
- IP do router que originou agregado

Community:

- Agrupa rotas com propriedades comuns
- Permite aplicar políticas ao nível de grupo
- Predefinidas: no-export, no-advertise, internet
- Formato geral: ASnumber:Cnumber

6.7 Seleção de Caminho BGP

BGP seleciona apenas um caminho como melhor, pela ordem:

1. Maior Weight (Cisco)
2. Maior Local Preference
3. Caminho originado localmente
4. Caminho mais curto (AS-PATH)
5. Tipo de origem menor (IGP < EGP < incomplete)
6. MED menor
7. Caminho externo sobre interno
8. Vizinho IGP mais próximo

6.8 MP-BGP (Multi-Protocol BGP)

Extensão do BGP:

- Transporta informação de routing sobre outros protocolos/famílias:
    - IPv6 Unicast
    - Multicast (IPv4 e IPv6)
    - 6PE (IPv6 sobre backbone MPLS IPv4)
    - MPLS VPN (IPv4 e IPv6)
    - Layer 2 VPN

Novos Atributos:

- **MP_REACH_NLRI**: destinos alcançáveis com next-hop
- **MP_UNREACH_NLRI**: destinos não alcançáveis
- Contém: AFI/SAFI, Next-hop, Reachability information

Negociação de Capacidades:

- Mensagem OPEN com parâmetro CAPABILITIES
- Contém: Multi-Protocol extensions (AFI/SAFI), Route Refresh, Outbound Route Filtering

6.9 Funcionalidades Avançadas

Private AS:

- AS numbers 64512-65535
- Usado quando cliente conecta a único ISP
- Removido pelo ISP com `remove-private-as`

Route Reflectors:

- Reduz necessidade de full iBGP mesh
- Route reflector e seus clientes formam cluster
- Full IBGP mesh apenas entre route reflectors

BGP Synchronization:

- BGP não deve anunciar rota antes de todos os routers no AS aprenderem via IGP
- BGP espera que IGP propague rota dentro do AS

Redistribuição de Rotas:

- IGP por BGP: simplifica configuração, anuncia apenas redes internas
- BGP por IGP: faz routers internos conhecerem rotas externas, aumenta tabelas

BGP sobre Tunnels:

- Resolve conflitos BGP/IGP
- Túneis IP-IP configurados manualmente
- Vizinhança BGP via túnel
- Rede do túnel distribuída via IGP

Filtering e Route Maps:

- Controlo de updates BGP enviados/recebidos
- Baseado em: informação de rota, informação de caminho, communities
- Route maps: controlar/modificar informação de routing, definir condições para redistribuição

7. Layer 2 VPN (VXLAN e BGP EVPN)

7.1 Datacenter Topology

CLOS Topology (Spine-and-Leaf):

- Evolução da topologia three-tier
- Desenhada por Charles Clos em 1950
- Elimina necessidade de STP
- Maior estabilidade e escalabilidade
- **Leaf Layer**: camada de acesso com suporte Layer 3
- **Spine Layer**: camada de agregação, interconexão entre leafs
- IP underlay transport requer IGP (OSPF ou IS-IS)

7.2 VXLAN (Virtual Extensible LAN)

Características:

- Encapsula frames Ethernet Layer 2 em datagramas UDP/IP Layer 4
- Porta default: 4789
- VNI field com 24 bits (vs 12 bits do 802.1Q)
- Header 802.1Q original removido e mapeado para VNI

VTEP (VXLAN Tunnel Endpoint):

- Dispositivos edge na rede VXLAN
- Responsáveis por encapsulação/desencapsulação do header VXLAN

VXLAN Flood and Learn:

- Tráfego multidestino é flooded sobre VXLAN entre VTEPs
- Aprende MACs dos hosts atrás dos VTEPs
- Tráfego subsequente pode ser unicast
- Abordagem nativa F&L não é ótima (domínio broadcast atravessa limites Layer 3)

7.3 EVPN MP-BGP

Objetivo:

- Mitigar problema de VXLAN Flood and Learn
- Address family L2VPN EVPN

Características:

- Transporta informação VPN-aware Layer 2 (MAC) e Layer 3 (IP) sobre sessão MP-BGP
- BGP usado para anunciar/aprender endereços VTEP remotos
- VXLAN transporta para VTEP remoto específico

Relações BGP:

- Apenas internal BGP (Route Reflectors nos spines)
- eBGP entre private AS:
    - Todos os Leafs num único private AS
    - Cada Leaf num private AS

EVPN Route Types:

Route Type-2 (MAC/IP Advertisement):

- Anuncia endereço MAC e IP de dispositivo remoto

- Respective next-hop
- EXTENDED_COMMUNITY: tipo de encapsulação e route target
- Enviado quando Leaf aprende novo endereço MAC

Route Type-3 (Inclusive Multicast Ethernet Tag):

- Define next hop para unknown unicast, multicast e broadcast
- PMSI Tunnel attribute define tipo de túnel
- Para EVPN com VXLAN: tunnel type é "Ingress Replication"
- Enviado quando novo Leaf (BGP peer) é adicionado

Route Type-5 (IP Prefix):

- Anuncia prefixos de rede IP
- Usado para Layer 3 VPN sobre EVPN com VXLAN

8. MPLS e Traffic Engineering

8.1 Traffic Engineering

Network Engineering:

- Construir rede para transportar tráfego previsto
- Problema: padrões de tráfego impossíveis de prever
- Routing baseado em destino não aproveita recursos ao máximo

Traffic Engineering:

- Manipular caminho do tráfego para ajustar à rede
- Pode ser feito com custos de protocolos routing ou MPLS
- Aumenta eficiência de recursos de largura de banda
- Previne links sobre-utilizados enquanto outros estão sub-utilizados
- Garante caminho mais desejável para algum/todo o tráfego

8.2 MPLS (Multiprotocol Label Switching)

Conceitos:

- Pacotes são labeled na fonte com label do primeiro hop
- Cada router toma decisão de forwarding independente baseada em label
- Simplifica processo de routing em routers

Vantagens:

- Simplificação do routing
- Capacidade de Traffic Engineering
- Simplificação de gestão de rede (protocolo único)

Domínio MPLS:

- Edge Routers: classificam pacotes, atribuem labels
- Core Routers: encaminham baseado em labels

8.3 Fundamentos MPLS

FEC (Forwarding Equivalence Class):

- Grupos de pacotes encaminhados sobre mesmo LSP
- Determinado na edge da rede MPLS

LSP (Label Switched Path):

- Caminho através da rede MPLS
- Frequentemente chamado "MPLS tunnel"
- Headers do payload não são inspecionados dentro do LSP

LSR (Label Switching Router):

- Router que implementa MPLS
- Data plane: IP Forwarding Table + Label Swapping Table

Label:

- Campo de 20 bits com valor do label
- Exp:

Continue

10:46 AM

3 bits (experimental)

- Stack: 1 bit (bottom of stack)
- TTL: 8 bits (independente de IP)
- Inserido entre headers layer 2 e layer 3 (PPP, Ethernet)
- Em ATM: campos VPI/VCI
- Em Frame Relay: campo DLCI

Label Stack:

- Múltiplos labels organizados em stack
- Labels internos: designam serviços, FECs
- Label externo: switch packets no core MPLS
- Bottom of Stack (S) bit: 1 para última entrada, 0 para outras

Operações:

- **PUSH**: adicionar label
- **SWAP**: trocar label
- **POP**: remover label

PHP (Penultimate Hop Popping):

- Penúltimo hop remove label
- Reduz carga no Label Edge Router
- Evita POP + IP Lookup no último router

LSP Merge:

- Múltiplos LSPs podem convergir num único LSP

LSP Hierarchy:

- Via label stacking
- Labels podem ser empilhados para suportar múltiplos serviços

8.4 Protocolos de Distribuição de Labels

Unconstrained Routing:

- **LDP (Label Distribution Protocol)**
  - RFC 5036
  - Caminho escolhido baseado em shortest path do IGP
  - Distribuição dinâmica de label binding
  - Descoberta de LSR
  - Transporte confiável com TCP
  - Manutenção incremental de tabelas

Constrained Routing:

- Constrained por definição explícita de caminho e/ou requisitos de performance
- **RSVP-TE (RSVP with Traffic Engineering)**
  - RFC 3209
  - Evolução do RSVP para suportar TE e distribuição de labels
- **CR-LDP (Constrained-based Routing LDP)**
  - RFC 3212
  - Evolução do LDP para suportar constrained routing
  - Deprecated!

MPLS VPN:

- MP-BGP usando address family VPN IPv4

8.5 LDP (Label Distribution Protocol)

Mensagens:

Discovery Messages:

- Hello Messages (UDP) para endereço multicast "all-routers" (224.0.0.2)
- Anunciam presença de LSR na rede
- Sessão LDP estabelecida sobre TCP após descoberta

Session Messages:

- Initialization: estabelece sessão
- KeepAlive: mantém sessão
- Porta well-known LDP: 646 (TCP e UDP)

Advertisement Messages:

- Address Messages: anuncia endereços de interface
- Address Withdraw: retira endereços previamente anunciados
- Label Mapping, Label Request, Label Abort, Label Withdraw, Label Release

Notification Messages:

- Informação advisory e sinalização de erros

Operação:

1. Hellos periódicos em interfaces com MPLS habilitado
2. Router com IP maior inicia sessão LDP/TCP
3. Peers trocam initialization messages
4. Keepalives mantêm sessão ativa
5. Troca de label mappings após keepalive

LDP e Hop-by-Hop Routing:

- Cada router gera novo label e associa a destino
- Operations: push (entrada), swap (core), pop (saída)

8.6 RSVP-TE

Características:

- Evolução do RSVP
- Mapeia traffic flows sobre topologia física através de LSPs
- Requer informação de recursos e constraints da rede
    - Fornecida por extensões TE ao OSPF (RFC 3630) ou IS-IS (RFC 5305)

Novos Objetos LSP Tunnel:

- **Explicit Route**: série de sub-objetos (IPv4/IPv6 prefix, AS number)
- **Label Request**: em PATH, requer label para túnel/fluxo específico
- **Label**: em RESV, contém label único
- **Record Route**: em PATH e RESV, coleta informação detalhada do caminho
- **Session Attribute**: em PATH, define tipo e nome da sessão, valores de prioridade

Novos Tipos de Objeto:

- Session: LSP_TUNNEL_IPv4, LSP_TUNNEL_IPv6
- Sender Template: LSP_TUNNEL_IPv4, LSP_TUNNEL_IPv6
- Filter Specification: LSP_TUNNEL_IPv4, LSP_TUNNEL_IPv6

8.7 Traffic Engineering Extensions to OSPF

TE-LSA (Type 10 Opaque LSA):

- Scope: flooding de área
- Anuncia informação sobre links TE-enabled

Top-Level TLVs:

- **Router Address**: endereço IP estável do router (tipicamente loopback)
- **Link**: descreve link único com sub-TLVs:
    - Link type, Link ID
    - Local/Remote interface IP address
    - TE metric

- Maximum bandwidth, Maximum reservable bandwidth
- Unreserved bandwidth
- Administrative group

Utilizações:

- Monitorização de atributos de link estendidos
- Constraint-based source routing local
- Traffic engineering global

9. MPLS Layer 3 VPNs

9.1 MPLS VPN Conceitos

Perspetiva do Utilizador Final:

- Serviço Virtual Private IP
- Routing simples (default route para provider)
- Conectividade full site-site sem desvantagens usuais

Benefício para Provider:

- Escalabilidade

9.2 Terminologia

Customer Router (C):

- Conectado apenas a outros dispositivos cliente

Customer Edge (CE):

- Peers Layer 3 com Provider Edge (PE)
- Interface PE-CE: protocolo routing dinâmico (eBGP, RIPv2, EIGRP, OSPF) ou routing estático

Provider (P) Router:

- Core da rede provider
- Não participa no control plane para prefixos de clientes
- Label Switch Router (LSR): papel principal no core, label switching/swapping

Provider Edge (PE) Router:

- Edge da rede MPLS SP
- Tabelas de routing VRF separadas para cada grupo de utilizadores
- Contém tabela de routing global para rotas no core SP
- Label Edge Router (LER) ou Edge Label Switch Router (ELSR)

9.3 VRF (Virtual Routing and Forwarding)

Características:

- Instância separada da tabela de routing global
- PE routers mantêm tabelas de routing separadas:

- **Tabela Global**: rotas PE e P (talvez BGP), populada pelo IGP backbone
- **Tabela VRF**: routing e forwarding para um ou mais sites diretamente conectados

Associação:

- VRF associada a qualquer tipo de interface (lógica ou física)
- Interfaces podem partilhar VRF se sites conectados partilham informação de routing

Populamento:

- Localmente através de protocolos routing PE-CE
- Via anúncios MP-BGP que correspondem à VRF definida
- Contexto de routing separado para cada VRF

9.4 Route Distinguisher (RD)

Função:

- Diferenciar 10.0.0.0/8 em VPN-A de 10.0.0.0/8 em VPN-B
- Torna rota única

Características:

- 64-bit quantity
- Configurado como ASN:YY ou IPADDR:YY
- Puramente para tornar rota única
- Rota única: RD:IPaddr (96 bits) + máscara na porção IPAddr
- Clientes não veem rotas uns dos outros

Configuração:

```
ip vrf VPN-A
 rd 100:1
 route-target export 100:1
 route-target import 100:1
```

9.5 Route Target (RT)

Função:

- Controlar política sobre quem vê que rotas
- Criar/adicionar a lista de VPN extended communities para determinar que rotas são importadas por VRF

Características:

- 64-bit quantity (2 bytes type, 6 bytes value)
- Transportado como extended community
- Tipicamente escrito como ASN:YY
- Cada VRF 'importa' e 'exporta' um ou mais RTs

Operação:

- RTs exportados transportados em VPNv4 BGP
- RTs importados locais ao box
- VRF PE que importa RT instala rota na tabela de routing VRF
- Permite interconexão de VLANs diferentes importando/exportando outros RTs VPN
- Rotas privadas não devem conflitar

9.6 VPNv4 BGP

Traduções PE:

- PE traduz rotas em rotas VPN-v4
- Atribui RD e RT baseado em configuração
- Reescreve atributo Next-Hop (para loopback PE)
- Atribui label baseado em VRF e/ou interface
- Envia update MP-BGP para todos os vizinhos PE

Recepção PE:

- PE traduz para endereço IPv4
- Insere rota na VRF identificada pelo atributo RT
- Label associado ao endereço VPN-V4 será usado em pacotes para destino

9.7 MPLS/VPN Packet Forwarding

Entre PE e CE:

- Pacotes IP regulares

Dentro da Rede Provider:

- Label stack:
    - **Outer label**: "levar pacote ao egress PE" (IGP label, de LDP/RSVP)
    - **Inner label**: "levar pacote ao egress CE" (VPN label, de MP-BGP)
- MPLS nodes encaminham baseado no TOP label
- Labels subsequentes ignorados
- Penultimate Hop Popping um hop antes do egress PE

Processo:

1. Ingress PE recebe pacotes IP normais
2. PE faz IP Longest Match da VPN FIB, impõe stack <IGP, VPN>
3. Core routers encaminham usando outer label (IGP)
4. Penultimate PE remove IGP label (PHP - implicit-null)
5. Egress PE usa VPN label para selecionar VPN/CE
6. VPN label removido, pacote roteado para site VPN

9.8 Notas Importantes

Core:

- Não executa VPNv4 BGP
- Mesmo princípio pode ser usado para BGP-free core para rede IP

CE:

- Não sabe que está em MPLS-VPN

Labels:

- **Outer label** (IGP): de LDP/RSVP, levar pacote ao egress PE
    - Independente de MPLS-VPN
- **Inner label** (VPN): de MP-BGP
    - Para egress PE saber para qual VRF encaminhar