1)**Mobilidade:voz e dados**

Limitações da rede móvel:

-Heterogeneidade de múltiplas redes independentes

-Queda da ligação frequente

-Largura de banda limitada

Limitações impostas pela mobilidade:

-Não existe noção de mobilidade pelos sistemas e aplicações

-Problemas de manutenção de rotas nos routers

Limitações do dispositivo móvel:

-Pequeno tempo de vida da bateria

-Capacidades limitadas

Aldeia Global -> Tudo é digitalizado(suportado pela Internet), devido à crescente digitalização de todos os media, incluindo as redes móveis.

**Internet**-> Conj. auto-organizado de componentes autónomos interligados

- mais de 60000 redes autonomas

-TCP/IP

-funcionamento por comutação de pacotes

-mais de 200 milhoes de dominios registados

-Trafego comercial > trafego não-comercial

- Máquinas diferentes podem oferecer serviços diferentes

- Único meio bi-direccional que suporta comunicações (um para um: unicast-> email; um para vários: multi-cast -> electronic news)

**Estrutura real da Internet**

-Aparentemente hierárquica

\_BackBone ISP fornece serviço a ISP’s cada vez mais pequenos

\_ISP’s pequenos eventualmente fornecem serviços aos utilizadores

- Mas a hierarquia não é respeitada!

\_acordos de ligação privados

\_arranjos de melhoria de rede

\_todos fornecem serviços a utilizadores

\_fornecedores de serviço ligam-se a multiplos fornecedores

\_Utilizadores ligam-se a múltiplos ISP’s

**Dados vs Voz->**Comutação de pacotes

-Óptimo para informação em burst

\_Partilha de recursos

\_Não há tempo de restabelecimento de chamada

-Congestionamento excessivo:atraso e perdas

\_Necessita de protocolos para transferência de dados fiável, sem erros

-Fornece serviço de comutação de circuitos?

\_Para aplicações multimédia é preciso assegurar Largura de Banda e Atraso(problema incompletamente resolvido)

**Serviços de transporte(ISP) vs aplicações**

-Perda de pacotes

\_Algumas aplicações suportam perdas

\_Outras requerem 100% de transmissão

-Largura de banda

\_multimedia preciso do minimo pra ser efectivo

\_email, transf. Ficheiros, usam a que conseguirem

-Temporização

\_jogos requerem baixos atrasos

\_aplicações sem requisitos de tempo real não apresentam limites estritos no atraso fim–a-fim

**Aplicações elásticas**

Traferências de dados interactivas (e.g. HTTP, FTP)

-Sensíveis ao atraso médio, não a pontos raros

Bulk data transfer(mail, news...)

-não são sensíveis ao atraso

-Best effort funciona

**Aplicações inelásticas**

Interativas:

-são sensíveis ao atraso dos pacotes (telefonia)

-Garantias de atraso máximo são necessárias

Não-Interactivas:

-Adaptam-se a maiores gamas de atrasos(streaming)

**2)BGP**

BGP4 foi lançada em 1993 e é hoje o protocolo que assegura conectividade de Internet.

Maioritariamente usado para routing entre Sistemas Autónomos (network com uma única administração)

**AS Numbers**

RFC 4271 define 2-bytes para um AS:

-Privado -> 64512 até 65535

-Publico -> 1 até 64511

\_39000+ já estão alocados

\_Será necessário expandir para 4-bytes

RFC4893 define suporte BGP para AS de 4-bytes

-A partir de 1 Janeiro de 2009.

-São divididos em 2 words de 16 bits:

\_<higher2bytes in decimal>.<lower2bytes in decimal>

-Example: AS 65546 -> “1.10”

-Cannot a “flag day” solution

**BGP Neighbor Relationships**

**-**configurado manualmente nos routers pelo admin

-Cada sessão corre sobre TCP (porta 179)

-Peers partilham todas as suas rotas na primeira ligação

-Só existem updates quando há uma mudança de topologia da rede ou na política de encaminhamento

-BGP peers trocam mensagens KEEPALIVE entre si (prevenir longos periodos de inacividade)

**External and Internal BGP**

IBGP – ligar a routers no mesmo AS

EBGP- ligar a routers de diferentes AS

-Um router BGP nunca transmite um caminho de um IBGP peer para outro IBGP a não ser que seja o melhor caminho (excepção quando é um route-reflector)

-O BGP encaminha as rotas aprendidas por um EBGP peer para todos os EBGP e IBGP peers

-IBGP Mesh->os routers IBGP num AS têm que manter uma sessão IBGP com todos os restantes no AS.

­\_Para obter informação completa das rotas sobre as redes externas

\_A maior parte das redes usam um IGP -> OSPF

\_Existem métodos para reduzir a complexidade do IBGP Mesh (Route reflectors, private AS...)

**Single-home (or Stub) AS**

-AS têm um único border router

\_Acesso único à Internet

\_Único ISP

**Multi-homed Non-transit AS**

-Mais que um border router

\_Acessos únicos à Internet

\_Vários ISP’s

-Não transporta trafego de outros AS

**Multi-homed Transit AS**

-Igual ao anterior mas transporta trafego de outros AS

**Path Vector**

-BGP é um protocolo Path-vector

-Embora seja essencialmente um distance-vector que transporta uma lista dos AS atravessados pela rota

\_fornece detecção de loop

-Um speaker EBGP adiciona o seu AS a esta lista antes de encaminhar a rota para outro peer EBGP.

-Um speaker IBGP não anuncia na lista porque está a enviar a rota com o mesmo AS

\_Lista dos AS não deve ser usada para detectar loops IBGP

**Path vectors**

Cada router sabe as rotas de todos os outros

**BGP Messages**

OPEN -> para estabelecer a sessão BGP

UPDATE -> para informar atualizações de rotas para outros sistemas BGP, permitindo que os routers possam construir uma visão consistente da topologia da rede, usando o TCP para garantir uma entrega confiável; essas mensagens podem retirar rotas inviáveis da tabela de roteamento e simultaneamente informar uma nova rota.

NOTIFICATION -> quando é detectado um erro de protocolo; a sessão BGP é fechada

KEEPALIVE -> são trocadas as mensagens quando o periodo de keepalive é excedido.

**BGP Attributes**

-É a métrica usada para descrever as caracteristicas do caminho BGP

-Os atributos estão nas mensagens de update:

-Well-known Mandatory

\_AS-path, Next-hop, Origin

-Well-known Discretionary

\_Local Preference, Atomic Aggregate

-Optional Transittive

\_aggregator, community, AS4\_agreggator, AS4\_path.

-Optional non-transitive

\_se o vizinho não suportar o atributo, é apagado

\_Multi-exit-descriminator

-Cisco-defined (local to router)

\_peso

**AS-path and Origin Attributes**

AS-path:

-Quando um anúncio de rota passa por um AS, o nº do AS é adicionado à lista de AS, como que a rota tivesse percorrido o AS.

Origin:

-Indica como é que o BGP aprende uma qualquer rota em particular

-IGP / EGP / Incomplete (origem desconhecida)

**Next-Hop Attribute**

EBGP next-hop é o IP usado para atingir à rota anunciada.

Para o EBGP, o next-hop address é o IP da conecção entre os peers.

Para o IBGP, o EBGP next-hop address é carregado no próprio AS

**Local Preference Attribute**

É usado para escolher um ponto de saida do AS local.

Se existirem multiplos exit points, o atributo é usado para escolher o exit point de uma rota específica.

**Atomic Aggregate and Aggregator Attributes**

Atomic aggregate

-É usado para alertar routers que certas rotas foram agregadas numa rota mais pequena.

Aggregator

-Forneçe informação sobre qual AS fez a agregação e o IP do router que originou o agregado

**Multi-Exit Discriminator Attribute (MED)**

É usado como uma sugestão para um AS externo.

O AS externo que recebe o MED pode usar outros atributos BGP para selecionar a rota.

Um valor mais pequeno na métrica é preferível.

MED é desenhado para influenciar chegada de trafego.

**Weight Attribute**

É definido pela Cisco.

Não é anunciado aos routers vizinhos

Se o router tiver mais que uma rota pro mesmo destino, a rota com o maior Peso é preferida.

**Community Attribute**

Usado por conjuntos de rotas que partilham propriedades.

Os atributos predefinidos são:

-no-export – Não anunciar esta rota aos pares EBGP

-no-advertise – Não anunciar esta rota a nenhum peer

-Internet – Anunciar a toda a Internet

Formato é Asnumber:Cnumber (300:1, 200:8)

**BGP Path Selection**

BGP pode receber vários anuncios da mesma rota de muitas fontes.

Selecciona um caminho como o melhor.

Coloca o caminho na IP routing table e propaga-o aos vizinhos. O critério é:

-Maior Peso;

-Maior Local preference;

-Caminho que é originado localmente

-Caminho mais pequeno

-Mais pequeno tipo de origem(IGP<EGP<Incomplete)

-MED mais pequeno

-prefere o external path ao internal path

-vizinho IGP mais perto

**Multi-Protocol Border Gateway Protocol (MP-BGP)**

-Extensão do BGP

-Encaminha informação de routing sobre outros protocolos

\_Ipv6 Unicaste

\_Multicast (Ipv4 e Ipv6)

\_6PE – Ipv6 sobre Ipv4 MPLS backbone

\_Multi-Protocol Label Switching (MPLS) VPN

-Multi-Protocol Reachability Information (NLRI)

**MP-BGP Attributes**

Novos atributos non-transitive e opcionais

-MP\_REACH\_NLRI

-MP\_UNREACH\_NLRI

-Address Family Information (AFI)

\_Identifica informação sobre NLRI

-Next-hop information

**MP-BGP Negotiation Capabilities**

OPEN message contem agora o parametro CAPABILITIES

-Multi-Protocol extensions (AFI/SAFI)

-Route Refresh

-Outbound Route Filtering

**MP-BGP New Features for IPV6**

IPv6 Unicast

IPv6 Multicast

IPv6 and label (6PE)

IPv6 VPN (6VPE)

**Advanced BGP->(Em falta):**

**-Private BGP AS**

**-BGP AS Routing Policies**

**-BGP Synchronization**

**-BGP Route Reflectors**

**-Routes Redistribution**

**-BGP Neighborhood Resilience**

**-BGP and IGP conflicts**

**-BGP over Tunnels**

**3)Redes acesso**

**Estrutura da rede**

Sistemas autónomos (AS)

-Encaminhamento intra-domínio

-Políticas internas próprias

-Podem não usar métricas iguais

-protocolos: RIPv2, OSPFv2

Interligação de Ass

-Encaminhamento inter-domínio

-Informação de conectividade

-protocolos: BGP

**MAN (Rede metropolitana)**

Conceito que está a retomar importância (antes DQDB; agora Ethernet, 802.16,...)

Situa-se entre a LAN e a WAN apresentando características de ambas

Pretende servir uma área geográfica para além do âmbito da LAN, mas restringida a uma comunidade específica, tipicamente uma cidade.

**Rede de núcleo (Core)**

Grande capacidade de transporte

Transporte diferenciado de vários tipos de tráfego (QoS)

Elevada tolerância a falhas

-Reencaminhamento de tráfego, contornando pontos de falha

Evolução aponta no sentido da generalização das tecnologias ópticas

**LAN – Local Area Network**

Infra-estrutura de rede de pequena/média dimensão para comunicação de dados entre computadores e outros equipamentos, para partilha de:

-Servidores (FTP, WEB, Mail, ...)

-Impressoras, unidades de backup, etc.

-Acesso à Internet

-Elementos de segurança (Firewalls, IDS, etc.)

Interligam computadores num mesmo edifício ou num conjunto de edificios próximos:

-Escritório

-Edifício/pequeno nº de edifícios

São normalmente implementadas com tecnologia Ethernet

São redes de altos débitos (>=100Mbps) com segmentos físicos de pequena dimensão (metros)

Rede sob administração de uma única entidade

**Rede de acesso**

Estabelece a ligação entre a rede local/equipamento terminal e a rede de transporte(Core/Núcleo)

Segmento de rede onde se identifica um grande nº de tecnologias

Difícil distinção entre Rede de Acesso e Metropolitana

Vulnerável a ataques de segurança e a avarias:

-Grande capacidade e infra-estrutura física mais exposta

-Acessos individualizados, sem mecanismos fortes de protecção contra falhas (redundâncias)

Com o actual desenvolvimento tecnológico a secção da rede de acesso é aquela onde os recursos são mais escassos (QoS)

**Tendências de evolução**

O transporte de IP na rede de acesso apresenta um elevado crescimento;

As expectativas de crescimento da utilização de fibra óptica até ao cliente (FTTH) não se cumpriram;

A introdução da banda larga no acesso tem-se feito ainda com a utilização do cobre instalado (xDSL), especialmente para o mercado residencial e utilizando as redes de distribuição de canais de televisão (CATV);

A tecnologia Ethernet também se está a expandir, quer via rádio (WLAN), quer como infra-estrutura de acesso dos Operadores/ISP

**Outras redes**

PAN – Personal Area Network

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

SAN – Storage Area Network

**IP sobre tecnologias de acesso**

Meio físico fixo

-Cobre

\_TDM comutado (POTS,RDIS)

\_xDSL

-Coaxial

\_CATV

-Fibra

\_ATM

\_SDH

-Misto

\_TDM dedicado (Nx64Kbps,PDH,SDH)

\_Frame Relay

\_ATM

Meio físico rádio

-WLAN 802.11 (PWLAN), GSM, UMTS, 802.16

Misto

-Ethernet

**Acesso banda-estreita (Dial-up)**

Modem para a banda da voz converte os dados em sinais eléctricos na banda dos 200Hz aos 3,4KHz

-Bandas limitadas pela utilização de gama de frequencias reduzida

Impossibilidade de utilização do serviço de voz enquanto utilizando dados.

**xDSL: Digital Subscriber Line**

Princípio:

-Re-utilização da infra-estrutura de cobre existente, normalmente utilizado para o serviço de voz fixo (analógico no acesso), para acessos de banda larga a serviços de dados

\_Maior capacidade que a dada pelos modems analógicos convencionais

\_Utilização das frequências acima da banda base para transmissão de sinais digitais sobre pares de cobre telefónicos

Meio físico dedicado desde o operador até ao cliente

Utilização de ATM como tecnologia de transporte (nível 2)

Resultado da evolução

-Metodologias de codificação

-Filtros analógicos e digitais

-Qualidade dos cabos da rede telefónica

Possibilidade de atribuição de um endereço público permanente

Capacidade de “Sempre ligado”

**Elementos de rede ADSL**

(CLIENTE)Modem ADSL ou ATU-R (ADSL Termination Unit - Remote)

-Elemento de cliente,para acesso à rede

-Outros elementos

\_IAD (Integrated Access Devices)

\_NIC ADSL

\_RGw (Residential Gateway)

(OPERADOR)DSLAM: Digital Subscriber Line Acces Multiplexer

-Concentração dos dados de múltiplas linhas DSL para ligação à rede de núcleo

-Contém vários Modem ADSL formando pares com os Modem ADSL dos clientes (ATU-C: ADSL Termination Unit - Central)

BBRAS: Broadband Remote Access Server

-Termina ligações para o cliente (PPP) e para a rede (L2TP)

-Routing e QoS

-Contém cliente AAA

Servidor AAA: Authentication, Authorization e Accounting

-Desempenha funções de Autenticação, Autorização e Contabilização

**Tipos de xDSL**

ADSL

-Asymmetric Digital Subscriber Line

-1 par

-Até 24 Mbps downstream, 3.3 Mbps upstream (ADSL2+)

-Aplicações residenciais

SDSL

-Symmetrical Digital Subscriber Line

-1 par

- >0.768 Mbps em cada direcção (1/2Mbps in 3Km)

HDSL

-High bit-rate Digital Subscriber Line

-2 pares

-2 Mbps em cada direcção, utilizando um ou dois pares de cobre

-Até 2,4 Km

VDSL

-Very high Speed Digital Subscriber Line

-51.84 Mbps downstream, 16 Mbps upstream

-Utilização de fibra nos segmentos iniciais (Fibre-to-the-Curb (FTTC), Fibre-to-the-Node (FTTN), or Fibre-to-the-Basement/Business(FTTB))

**xDSL: bridging**

Vantagens:

-Simples de compreender e configurar os CPE

-Requer CPE mais simples; Fácil de instalar

-Multi-protocolo (CPE não observa os protocolos de nível de rede)

Desvantagens:

-Requer broadcast para funcionar (bridges, ARP, ...)

-Inseguro (IP hijacking e ARP spoofing challenges)

-Apenas um utilizador por acesso

**PPP (Point-to-Point Protocol) RFC 1661**

Protocolo nível 2

Comum nos acessos Dial-Up aos ISPs

Necessário para a transmissão de IP sobre linhas série

Possibilita a identificação do utilizador, integrando autenticação por login/password (protocolos CHAP ou PAP)

Proporciona:

-Negociação de parâmetros da ligação

-Capacidade de transporte de informação sobre linhas série

-Segurança

-Gestão de endereços IP

-Contabilização

Duas componentes:

-LCP: Link Control Protocol

-NCP: Network Control Protocol

**PPPoE (Over Ethernet)**

Modo mais utilizado pelos ISPs ADSL

Requisitos:

-Ligar vários equipamentos na rede local sobre a mesma infra-estrutura de acesso (CPE)

-Efectuar controlo de acessos e contabilização de forma semelhante ao efectuado nos acesso Dial-up

\_Adição do conceito de username/password (login/logoff) à rede DSL: autenticação, sessão e contabilização

\_Contrário ao conceito de always-on, flat-rate, ...

-Baixo custo (apenas mecanismo de bridging no CPE)

-Acesso a serviços VPN (disponível utilizando L2TP no BBRAS)

Permite:

-Controlar o acesso de uma forma que os utlizadores já conhecem

-Controlo e contabilização por utilizador e não por local:estabelecimento de sessões PPP com autenticação

-Utilização de Ethernet na LAN

-Selecção do ISP a utilizar

CPE configurado em modo bridging RFC1483 puro

-Apenas um PVP/PVC é utilizado para todos os terminais por detrás do CPE

\_Multiplas sessões PPP sobre o mesmo PVC

-CPE não faz NAT ou é servidor DHCP

Definição de endereços IP efectuada pelo router concentrador (BBRAS) ou, se utilizando L2TP, pelo gateway do cliente

Requer a instalação de software específico em cada um dos terminais

**CATV**

**Acesso CATV**

Rede comum

-Elevado nº de casas com acesso à rede

-Rede mista composta por cabo coaxial e cabo óptico

\_HFC: Hybrid Fiber Coaxial

-Rede uni-direccional para a difusão de canais de televisão

-Evolução para infra-estrutura bi-direccional para o transporte de dados

\_Utilização inicial de outra rede (p.ex. telefónica/modem) para o canal de retorno

-Canal descendente diferente do canal ascendente

\_Banda larga descendente

\_Banda estreita ascendente

-Até 1GHz de largura de banda

**Dados sobre CATV**

Utilização de rede HFC de distribuição de canais de tv analógica para o transporte de voz

-Solução destinada ao mercado residencial

Rede HFC

-Rede de distribuição de sinais bidireccional (upstream e downstream) partilhada, com infra-estrutura híbrida óptica e coaxial

-Todos os terminais ligados numa mesma rede recebem todos os sinais sendo necessários mecanismos de segurança que garantam a necessária privacidade

-Rede não securizada principalmente contra falhas de energia

Standard DOCSIS (Data-Over-Cable Service Interface Specification)

-Especificação da utilização de canais de TV para o transporte de tráfego digital (dados, voz e vídeo digitais)

\_Downstream: vários canais de 6MHz (8MHz para o EuroDOCSIS) em frequências acima dos 50 MHz, disponibilizando cada um 27 Mbps partilhados

\_Upstream: frequências entre 5 e 42MHz, com canais de 1,8MHz, disponibilizando cada um 1,8Mbps partilhados (largura de banda assimétrica)

-A banda disponibilizada é partilhada por todoso os utilizadores activos no mesmo canal (qualidade depende do nº de utilizadores em simultâneo)

-Utilização de esquema de endereçamento (unicast e multicast) e de mecanismos de autenticação robustos para os Cable Modems, utilizando certificados digitais.

**Elementos de rede**

Cliente

-CM: Cable Modem

-Cable router (opera em modo IP routing)

-Set-Op Box (STB)

Operador

-CMTS: Cable Modem Termination System

\_Gestão de pilhas IP (IP Pools)

\_Gestão dea atribuição de recursos (MAC) no upstream

\_Adaptação de meios físicos e lógicos

**WLAN**

**Acesso WLAN**

Objectivo:

-Disponibilizar acesso sem fios a serviços do tipo Internet, utilizando mecanismos e protocolos de rede local (WLAN – Wireless LAN)

Vantagens:

-Mobilidade

-Disponibilidade

-Baixo custo de instalação da infra-estrutura de suporte

-Facilidade de instalação e utilização no terminal

Disponibilização em áreas públicas

-PWLAN: Public Wireless LAN

-Constituição de Hot-Spots

**Oportunidade**

As redes wireless formam:

-Um complemento importante às redes fixas, aumentando a área de cobertura de rede.

-Um complemento ao serviço 2,5G

\_Aproveitando o lento desenvolvimento do GPRS

-Uma alternativa às redes móveis 2,5G e 3G

\_Aproveitando o atraso no lançamento do UMTS (Preparação do mercado para o 3G / Contribuição na evolução para o 4G)

Existem segmentos de mercado com apetência para este tipo de serviço

**Partilha de infra-estrutura**

Baseada na capacidade de alguns AP suportarem multiplos SSID

Mapeamento SSID <-> VLAN

Cada SSID/VLAN pode ter o seu próprio processo de autenticação e políticas de QoS

**Componentes PWLAN**

AZR – Access Zone Router

-Routing IP

-Acesso WAN (xDSL, E1, FR, …)

-Gestão de endereços IP do Hot Spot (Servidor DHCP)

\_Detecção de utilizadores não activos (Utilização dos lease time do DHCP e do endereço IP para determinar a localização do terminal)

**ATM – Asynchronous Transfer Mode**

ATM standard (defined by CCITT) é amplamente aceite como o modo de

operação para a comunicação.

ATM é uma forma de comutação celular com pacotes pequenos de tamanho fixo

5bytes-Header / 48bytes-Payload

-É organizado como uma hierarquia

\_Equipamentos conectam-se a redes via UNI (User-Network Interface)

\_as conexões entre redes são feitas através do NNI(Network-Network Interface)

-ATM é orientado à conexão

\_A conexão precisa estar estável antes de fazer chamadas.

-Maior parte das redes ATM correm em fibra óptica com taxas de erro muito pequenas.

-ATM suporta acessórios de baixo custo

**ATM Connections**

2 níveis:

-virtual path connections

-virtual channel connections

2 campos no Header:

-virtual path identifier VPI

-virtual channel identifier VCI

**ATM Protocol Architecture**

ATM Adaptation Layer (AAL) – protocol para segmentar os dados para colunas do ATM?

**ATM Service Categories**

CBR – Constant Bit Rate – T1 circuit

RT-VBR – Real Time Variable Bit Rate – Real-time videoconferencing

NRT-VBR – Non Real Time… - Multimedia email

ABR – Available Bit Rate – Browsing the Web

UBR – Unspecificied Bit Rate – Background file transfer

**QoS, PVC, and SVC**

Os requisitos QoS são manipulados no momento da conexão e visto como parte de sinalização.

ATM fornece conexões virtuais permanentes

e conexões virtuais *switched*.

-Permanent Virtual Connections (PVC)

\_conexões permanentes configuradas manualmente pelo gestor da rede.

-Switched Virtual Connections (SVC)

criado e lançado *on demand* pelo usuário final via procedimentos de sinalização.

**ETHERNET**

Redes baseadas em ligações ponto-a-ponto (P2P)

-por exemplo: Ethernet in the First Mile (IETF EFM)

Redes baseadas em comutação Ethernet:

-Multiplos níveis de comutadores Ethernet (nivel 2)

**Novos Protocolos**

IEEE 802.1s (MTP – Multiple Spanning Trees)

-proposto para permitir mais que um loop-free path numa VLAN

IEEE 802.1w (RRSP – Rapid Reconfiguration of Spanning Tree)

-implementa um algoritmo de rápida convergência (+/- 1 seg)

-ainda não se aproxima do SDH/SONET(50 ms)

IEEE 802.17 (Resilient Packet Ring working group)

-defende um protocol de protecção de chamada que fornece <50 ms failover

IEEE 802.3ad (Link aggregation)

-fornece a capacidade de usar dois links físicos entre dois nós, o que permite técnicas de balanço e rápida protecção do link.

**Limitações da Ethernet**

Escabilidade para suportar um nº elevado de clientes

Garantia de parâmetros de fiabilidade “carrier-grade” suportada eficazmente por mecanismos de recuperação de falha

Mecanismos de controlo de qualidade de serviço poderosos

Segurança – separação segura do tráfego de clientes

Comprimento máximo das linhas no acesso, a baixo custo

**4)MPLS**

**Substitution of SDH/SONET circuit-switching transport network:**

Removing:

-Alocamento da Largura de banda no circuit-switching inflexível

Keeping:

-Orientado à conexão

-Performance determinista e QoS

-Alta resiliência e avaliação baseada em:

\_In-band OA&M

\_Protecção com 50ms de recuperação

-Segurança

-Modelo operacional centralizado, Simples

**IP networks over ATM**

IP routers são interligados por uma rede ATM

As ligações são feitas através de virtual circuits ou virtual paths na rede ATM

É necessário gerir duas camadas protocolares

**MPLS networks**

O label dos pacotes é o label do primeiro salto

Vantagens:

-Simplificação do processo de routing dos pacotes nos routers

-Trafego equivalente ao ATM

-Simplificação da gestão da rede (Unica camada protocolar)

**IP/MPLS improves:**

Removing:

-Conectividade IP;

-QoS limitada;

Keeping:

-IP Statistical Multiplexing;

-Plano de controlo de IP dinâmico

Offering:

-Orientado à conexão;

-Gestão da largura de Banda eficaz com QoS;

-Alta Escabilidade;

**IP/MPLS**

FEC – Forwarding Equivalence Class – identifica o grupo de pacotes MPLS que são manuseados na mesma direcção;

LABEL – Identificador local do FEC;

LSR – Label Switching Router;

LER – Label Edge Router – interage com os devices fora do domínio, usando tecnologia IP

LSP – Label Switched Path – Caminho que o FEC atravessa pela rede MPLS;

LDP – Label Distribution Protocol – classifa FEC’s, distribui labels e mantem LSP’s

LFIB – Label Forwarding Information Base – Tabela criada por protocolos de routing e labels:

LSP tunneling – Explicita a rota LSP entre dois LSR’s que não estejam diretamente conectados;

Multi-level label stack – carrega os pacotes MPLS organizados numa stack LIFO;

**Discovery link and topology**

A tabela de routing IP é construida:

-LSRs e LERs esam protocolos de routing para descobrir a topologia de rede (OSPF, ISIS, BGP);

-CEs anunciam os seus endereços usando protocolos de routing na cloud MPLS;

Forwarding Information Base (FIB) é construida inicialmente sem informação de label

**Label Assignment**

FECs creation

-LSRs classificam com o mesmo FEC todos os pacotes manuseados na mesma direcção;

Allocate Labels

-Todos os LSRs alocam os labels locais para todos os destinos na tabela de routing IP (LIB e LFIB setup)

**Label distribution operation e LSP Establishment**

Discovery

-Basic Discovery – LSRs enviam link LDP Hellos (UDP) para os peers diretamente ligados.

-Extended Discovery – LSRs enviam LDP targeted Hellos (UDP) para um especifico IP peer

Session Establish and Maintenance

-Uma sessão TCp é estabelecida e mantida por mensagens periodicas Keep-Alive

LSP Establishment and Maintenance

-Downstream On-demand mode- Upstream LSR envia um label request message para o Downstream:

\_Ordered mode – LSR só responde quando receber o label do Downstream

\_Independent mode – LSR responde quando receber um request label qualquer

\_Unsolicited mode – Downstream LSR anuncia informação ao Upstream LSR unsilicited depois da sessão estabelecida, sem request;

Label retention mode

-Conservative mode

\_LSRs mantêm só as labels dos proximos saltos

\_Indicado para limitar o espaço para labels

-Liberal mode

\_LSRs mantêm todos os labels

\_Indicado para uma adaptação rápida às mudanças de rota

LFIBs são estabelecidos de acordo com as tabelas de routing e de Label

**Label Switched Path: virtual circuit with label switching**

Redes são organizadas em domínios;

Border routers inserem/cancelam labels;

Labels têm significado local (podem ser usados noutros links)

Distribuição dos labels é feita por um protocolo apropriado

**Labels**

Em algumas tecnologias Data Link (nivel 2), o label é dado pelos campos apropriados do seu header

-ATM technology: VPI (Virtual Path ID) e VCI (Virtual Channel ID)

-Frame Relay technology: DLCI (Data Link Connection Identifier) field

Noutras tecnologias Data Link (p2p, Ethernet), o label é inserido entre os headers da camada 2 e 3

**Constrained based Routing**

É o custo associado a cada link

Cada link tem um conj de atributos que representa a métrica de performance (O objectivo é determinar o caminho mais curto que nao viole as restrições a que está inserido)

Restrições podem ser: largura de banda, delay, prioridade, etc

-No caso da largura de banda, a restrição que é imposta ao algoritmo é que o caminho tem que ter, em cada conexão que atravessa, uma largura maior que um certo threshold.

Basic components

-Especificar restrições do path

-Extender a topologia para incluir informação das restrições

-Encontrar caminhos que não violem isso e optimizem alguma metrica

-Reservar recursos ao longo do path

-activar LSP ao longo do path (com a devida rota)

-Mapear trafego para os LSPs apropriados

**LSPs establishing protocols**

RSVP-TE – Resource Reservation Protocol – Traffic Engineering – Extensão do protocolo RSVP

CR-LDP (Constrained based Routing – Label Distribution Protocol) – Extensão do protocol LDP

Ambos permitem:

-A especificação da rota para o LSP

-Escolher os labels de cada link da rota

- Reservar recursos para o LSP

Rotas são previamente determinadas:

-Pela gestão (Traffic engineering)

-Por um protocolo tipo CR

**LDP – Label Distribution Protocol**

Distribuição dinâmica da informação dos labels

LSR discovery

Transporte confiável com TCP

Manutenção incremental das label swapping tables

Desenhado para ser extensível a mensagens de codificação TLV(Type-Lenght-Value)

Modos de comportamento são negociados durante a sessão inicial

- Label retention (liberal or conservative)

-LSP control (ordered or independent)

-Label assignment (unsolicited or on-demand)

**LDP Message Categories**

Discovery – usadas para anunciar e manter a presence de um LSR numa rede

Session – usadas para estabelecer, manter e terminar sessões entre peers LDP

Advertisement – usadas para criar, mudar e apagar label mapping para os FECs

Notification – usadas para fornecer informações de assessoria e sinalizar erros de informação

**A closer look at CR-LDP**

Define novos procedimentos e codificações TLV para:

-Explicit routing (perdido e estrito)

-Fixar rotas

-Especificar parametros de tráfego

\_Peak rate

\_Commited rate

\_Weight

\_Resource class or color

-LSP preemption (redefinir caminhos existentes para acomodar um caminho novo)

-LSP identifiers (LSPIDs)

**LSPs priorities**

O operador pode estabelecer diferentes prioridades para evitar que trafego “mais importante” bloqueie o “menos importante” se:

-Um novo LSP requer recursos que não existem na rede;

-Em situações de falhas (num link, p.ex.)

Cada LSP tem 2 prioridades: “setup Priority” e “holding Priority”

Existem 8 niveis diferentes de prioridade

Um LSP pode “roubar” recursos a LSPs com menor prioridade.

**MPLS – Major Drivers**

Fornecer IP VPN Services

-IP VPN service escalável – contruido uma vez e vendido muitas

-Managed Central Services – Construindo serviços de valor acrescentado e oferecendo-lhes através de VPNs

Tratando trafego na rede usando MPLS Traffic Engineering

-Fornecendo SLA/QoS mais apertado

-Protegendo a largura de banda

Integrando Infraestruturas Layer 2 & Layer 3

-Serviços Layer 2: Frame Relay e ATM sobre MPLS

-Imitar serviços layer 2 sobre uma infraestrutura layer 3 altamente escalável

**IP/MPLS Applications**

**MPLS-based VPN**

MPLS L3VPN – VPN-IP over MPLS

-VPN é uma rede segura IP-based entre sites distantes geograficamente que comunica de forma segura sobre um backbone partilhado;

-Perspectiva End user:

\_Virtual Private IP service;

\_Simple routing;

\_Conectividade site-site completa sem as habituais desvantagens (cost, configurations..)

-Maior vantagem para fornecedor- escalabilidade;

-MPLS VPNs fornece a capacidade de implantar e administrar um serviço Layer 3 VPN backbone para clientes empresariais;

MPLS L2VPN – Any Technology or Transport over MPLS

-Permite o uso da rede MPLS para fornecer conectividade entre clientes locais com redes Layer 2;

MPLS-TE

-Extende os protocolos IP existentes e usa as capacidade de forwarding da rede MPLS para fornecer TE

-Oferece capacidades explicitas de routing às redes MPLS

**VPN Routing and Forwarding Instance (VRF)**

PE routers mantêm tabelas de routing separadas

-Global routing table

\_Contem todas as rotas P e PE (talvez BGP)

\_Populosa pelo VPN backbone IGP

-VRF

\_Associada a um ou mais sites diretamente ligados (CE routers)

\_VRF é associado a qq tipo de interface

\_Interfaces podem partilhar o mesmo VRF se os sites conectados partilharem a mesma informação de routing

**Route target**

Cria ou adiciona a uma lista de comunidades VPN usada para determinar quais rotas são importadas pelo VRF

Controla a política de quem vê o que encaminha

64-bit (2bytes type, 6bytes value)

Cada VRF importa e exporta um ou mais RTs

-RTs exportados são transportados por VPNv4 BGP

-RTs importados são locais

O PE que importa um RT instala essa rota na sua tabela

**VPNv4 -> VPN routes for Ipv4**

No BGP para IP, 32-bit address+mask faz um único anuncio

No BGP para MPLS-VPN, 64-bit RD+32-bit address + 32-bit mask fazem um unico anuncio

Se a codificação da rota for diferente, precisa de uma diferente familia de endereços no BGP

O anuncio do VPNv4 transporta um label com a rota

**Terminology**

RR-Route Reflector

PE-Provider Edge Router

P-Provider Router

CE-Customer Edge Router

LDP-Label Distribution Protocol

LSP-Label Switched Path

RD-Route Distinguisher

RT-Route Target

**5) P2P Peer-to-Peer networks**

Explora a diversa conectividade entre participantes numa rede

Explora a largura de banda acumulada nos participantes da rede

Tipicamente usada para ligar nós em grande parte em ligações ad-hoc

-Partilhar ficheiros (audio,video,data)

-Alguns dados real-time, como trafego telefónico

Rede P2P pura

-Não há noção de clientes e servidores

-Nós iguais que funcionam tanto como clientes como servidores para outros nós na rede

**P2P Model**

Os recursos do peer são semelhantes aos dos outros participantes

Peers comunicam diretamente com outros peers e partilham recursos

P2P services:

-Computação distribuida

-Partilha de ficheiros

-Colaboração

-Plataformas

**Simple Peers**

Um simple peer é designado para servir um unico utilizador final, permitindo-o fornecer serviços através do seu dispositivo e consumir serviços fornecidos por outros peers na rede.

Contra outros tipos de peer, eles não são responsáveis por servir como intermediário na comunicação de outros peers ou servir informação a uma terceira parte para consumo de outros peers

**Rendezvous Peers**

Literalmente, rendezvous é um ponto de encontro

-No P2P, rendezvous peer fornece aos peers uma rede para descobrirem outros peers e recursos.

Pode aumentar as suas capacidades ao retirar informação de peers para uso futuro ou encaminhar discovery requests a outros rendezvous peers

-Estes esquemas tem o potencial de desenvolver capacidade de resposta, reduzir o trafego da rede e fonecer um melhor serviço aos simple peers.

Vai normalmente existir fora de uma rede de firewall privada. Pode existir por trás da firewall, mas tem que ser capaz de atravessa ra firewall usando um protocolo autorizado pela mesma ou um router peer fora dela.

**Router Peers**

Fornece um mecanismo para a comunicação entre peers separados da rede por uma firewall ou equipamento NAT.

É um bom intermediário de peers fora da firewall com um peer por trás da firewall e vice-versa.

Para enviar uma mensagem a um peer via router, o peer precisa primeiro determinar qual router peer é que vai comunicar com o peer destino.

**P2P e a sua organização em arquitecturas**

-Networking layer – Regular Internet IP protocols (communication type) – Routing, DNS (inf discovery) – TCP (inf. Transport)

-Data Access – Overlay Networks, P2P – Resource Location (DHT,central server) – Gnutella, FreeNet

-Service – Application interface – Messaging, Distributed Processing – Napster, SETI, Groove

User – User Communities, Google Circles, Collaboration, eBay, Google+. Facebook

**Centralized vs Distributed**

Centralized

-Existe um centralized server para o upload e download de ficheiros ou outras apps

Flooding/distributed

-Qualquer nó na rede P2P pode funcionar como peer servidor para down/upload

Hybrid

-É escolhido o cliente mais perto

-É usado load balancing

**Centralized Inf Systems**

Web search engine

-Google (p.ex.)

\_150 Biliões de pesquisas

\_24 Petabytes de dados

Vantagens

-Ranking global

-Rápido tempo de resposta

-Pesquisa eficiente

-Usa largura de banda limitada

Desvantagens

-Infraestrutura, administração, custo

-Escala limitada

-Ponto central de possivel falha

**Fully Decentralized Inf Systems**

P2P file sharing

-Gnutella

\_40000 nós, 3 Milhões de ficheiros

Vantagens

-Bom tempo de resposta

-Sem administração nem infraestrutura

-Não há ponto unico de falha

Desvantagens

-Alto tráfego na rede

-Sem pesquisa estruturada

-parasitismo

**Flooding**

Vantagens

-Sem ponto central de falha

-Estado limitado por nó

Desvantagens

-Pesquisa lenta

-Intensa largura de banda

**Hybrid/Hierarchical**

Vantagens

-Sem ponto central de falha

-Pesquisa mais eficiente

-Partilha de carga

Desvantagens

-Nós mais complexos

**Semi-Decentralized Inf Systems**

P2P music file sharing

-Napster

\_1,37 Milhoes de users

\_10 TeraByte de dados

Vantagens

-Partilha de recursos

\_cada nó “paga” a sua participação fornecendo os seus recursos

\_todos os nós funcionam como cliente e servidor

\_informação global com pouco investimento

\_descentralização do custo e admin

Desvantagens

-Servidor é unico ponto de falha

-Unica entidade controla o sistema

-Material copiado (ilegal)

**Structured vs Unstructured**

Unstructured P2P networks

-Formada quando os links overlay são distribuidos aleatoriamente

-Se um peer quer encontrar determinado dado na rede, é feito um flood na rede para encontrar quantos peers podem partilhar esse dado

Structured P2P networks

-Emprega um protocolo consistente que assegura que qualquer nó consegue procurar um peer com o ficheiro desejado, a não ser que seja mesmo muito raro.

-O tipo mais comum é o DHT (Distributed Hash Table)

\_Uma variante de hash consistente é usada para atribuir a propriedade de cada ficheiro a um peer, analogamente ao tradicional hash table que atribui uma chave a um array slot

\_Chord, Pastry, Tapestry, CAN, Tulip

**P2P Applications**

File sharing

-DirectConnect(centralized), Gnutella(flooding), BitTorrent(hybrid)

VoIP

-Using SIP(Session Initiation Protocol)

Streaming media

Instant messaging

Software publication and distribution

Media publication and distribution

-radio, video

**Routing**

Routing IP é centralizado ou automaticamente configurado sem problemas

P2P overlay network routes separately

-Topologia Virtual no topo dos links físicos da rede

-Nós entram e saem da rede dinamicamente e o uptime de cada nó é relativamente baixo

-A topologia pode mudar a qq momento

-O routing nestas redes é problemático

Tópicos para desenhar algoritmos de routing P2P

-Escalabilidade

-Complexidade

-Anonimidade

**Routing in Gnutella**

Para entrar na rede, o cliente precisa de saber o endereço de pelo menos um nó existente na rede

Depois de entrar pode fazer ping para encontrar endereços de outros nós

Cada cliente mantem conexão com cerca de 5 nós

Para pesquisar um recurso, envia um Query para cada nó conectado

-Quando o recurso é encontrado, o nome e o endereço é propagado ao longo do caminho

-o nº de nós que foram contactados pode ser controlado usando o TTL counter

-É possivel um tipo de routing simples para uma overlay network

Trabalha bem para redes pequenas/medias

**Searching in DHTs**

É necessário conhecer o nome exacto do file

**Routing through DHT**

Útil para a partilha de ficheiros ou outros dados numa rede P2P

Uma função hash toma uma string de bytes e retorna um nº que é gerado pela string

Chord é um bom exemplo de um algoritmo DHT

-todos os dados têm um identificador que na função hash vai gerar uma chave para um determinado recurso

-Se um nó precisar de um ficheiro, vai criar o hash do nome e envia o request usando a chave

Vantagens

-Garante que a resposta chega com um tempo Log(n)

-Pouca sobrecarga redundante

**Flooding vs DHTs**

Recall

-Flooding pode perder ficheiros

-DHTs quase nunca perde

Query complexity

-Flooding pode administrar uma logica single-site

-DHTs pode fazer agregados, selecções, equijoins, etc

Query Performance

-Flooding pode ser lento a encontrar dados

-DHTs é caro para publicar documentos com muitos termos

Solução Hibrida -> melhor dos dois mundos

-Flood-based (Search Popular Items)

-DHT (Search Rare Items)

**Security attacks**

Poisoning attacks

-ficheiros que contem dados diferentes do esperado

Polluting attacks

-inserir “maus” pacotes num ficheiro valido

Freeloaders

-Usar sem contribuir

Insertion of viruses to carried data

-download de ficheiros com virus

Denial of service attacks

-Ataques para a rede a correr muito lenta

**P2P Benefits**

Custo da partilha

Agregação de recursos

Fornece escalabilidade

Proporciona autonomia

Anonimidade

Dinamismo

Comunicação ad-hoc

**6) CDN and P2P**

O que é comum?

-Ambos reflectem um conj de problemas do modelo cliente-servidor

-São focados no conteudo e não nas comunicações interactivas

-Refletem overlays

**Overlay**

Consiste num software de routing instalado em sites seleccionados, conectados por tuneis ou links diretos.

Exemplos:

-Mbone, 6Bone

-P2P(Napster,FreeNet,Gnutella,Bittorrent)

-Cooperating Caches

-Server farms

-CDN(Content Distribution Networks)

**CDN Motivation**

IP based networks

Larga aceitação e crescimento explosive

-Sérios problemas de performance

Mais saltos entre o cliente e o WebServer -> mais congestionamento

Os mesmos dados são repetidos muitas vezes entre clientes e o WebServer

O servidor original é pequeno para o crescimento do nº de utilizadores

**What is CDN?**

Uma rede de servidores que enviam conteudo por intermedio de um site.

-Sem clientes nem servidores personalizados

-Sem pré-posicionamento

-Sem provisionamento manual

**CDN status**

Companhias a utilizar:

-Akamai, Digital Island, Speedera

Companhias a explorar:

-CNN, CNBC,...

Melhorar o tempo-resposta de um site

**Vantagens**

Melhor escalabilidade

Maior disponibilidade

Melhora tempo-resposta de uma “centraly managed solution”

Nós são desenhados para ser:

-auto-configuráveis

-auto-geridos

-auto-diagnosticados

-self-healing

**Desafios**

Distribuição, configuração e gestão

Segurança da aplicação

Desenvolvimento de modelos de programação consistente com a industria actual (J2EE)

**With CDNs**

Overlay network para distribuir conteudo de servidores para utilizadores

-Evita dados repetidos que congestionariam o trafego

-Reduz a carga do WebServer

-Tenta encaminhar à volta da rede congestionada

CDN não é cache!

**-**Caches são usadas por ISPs para reduzir o consumo de largura de banda, CDNs são usadas pelos fornecedores de conteudo para melhorar a qualidade do serviço aos utilizadores finais

-Caches são reactivas, CDNs são proactivas

**CDN Components**

Content Delivery Infrastructure;

Request Routing Infrastructure;

Distribution Infrastructure;

Accounting Infrastructure;

**7)VoIP**

Circuit switched systems

-Produtos baseados em TDM ainda trazem beneficios na industria

-Estão perto dos limites de custo e de eficiencia

-Obsoletos

Packet switched systems

-Serviços baseados em IP vão ser dominantes (SIP, VoiceXML)

-novas caracteristicas distribuidas entre gateways e media servers

Conversação é um ponto crítico

**RTP**

**Desvantagens do TCP**

Orientado à conexão (não apropriado para multicast)

Retem trafego (push)

Retransmissões não são convenientes para pouco trafego (aceita perdas)

Não há limite de tamanho de dados

**Desvantagens do UDP**

Não há garantias de conexão

Não há controlo de erro

Não há controlo de fluxo

**RTP**

Inclui RTP: transmissão em streaming e RTCP: mensagens de controlo

RFC1889-> formato das mensagens

Fornece serviços de:

-Identificação de pacotes, feedback, timestamping

-não dá garantias de envio ou QoS

**RTP session and cloud**

São interligados por relays, em que cada participante tem um identificador unico

**Light sessions**

Não há um controlo do grupo de participação

Os membros que tem dados pra enviar, simplesmente enviam-nos

Adequado para modelos multicast

**Types of RTP entities (Relays)**

Translators

-Modificam o formato dos dados

-não modificam SSRC

-Exemplos: multicast to unicast, coding, flow quality reduction

Mixers (SSRC field)

-Gera uma saida de varias entradas (CSRC field)

-Exemplos: audio mixer, video PiP

**RTCP**

Associado ao RTP, envia toda a sessão em multicast (um endereço multicast por sessão, partilhado por pacotes RTP e RTCP)

Essencial para multicast

**RTCP Protocol**

Fornece informação sobre a qualidade de recepção

-A emissores e receptores;

-Informação da QoS

\_packet info: loss, delay, jitter

\_end-system info

Identifica cada participante

Calcula o nº de fontes

Controlo mínimo de sessão

**Tipos de pacotes RTCP**

Sender Report

Receiver Report

Source Description

Bye

APP

**RTP limitations**

Não guarda recursos

Não tem garantias QoS

Não suporta controlo de trafego

Deve trabalhar com RSVP e ATM para garantir QoS

**Standard H.261**

Codigo de video semelhante ao MPEG

Assume perdas

Se perder dados:

-Resincroniza com o proximo grupo de blocos (GOB)

-Reconstroi erros no descodificador

**VoIP**

**Signalling**

É o processo de interação entre nós e chamadas

-serve para o control de chamada

-origem e destino tem de aceitar condições de estabelecimento

SS7 é o signalling usado no PSTN

Também existe em SIP,Megaco,H.323...

**What is VoIP?**

Não é um protocolo

-Conj de protocolos e equipamentos que permitem codificação, transporte e routing de chamadas audio em redes IP

Exemplos:

-PSTN -> VoIP -> PSTN

-VoIP Native -> PSTN

-VoIP Native -> VoIP Native

Vantagens:

-redução de custo e largura de banda

-Integração de redes de voz e de dados

**SIP**

Protocolo para estabelecer sessões na internet, generico e pouca complexidade

Objectivo:

-Permitir a reutilização de protocolos existentes

-Alternativa ao H.323

\_Suporta novos serviços

\_Escalável

\_Extensível

Permite criar modificar e terminar sessões multimedia com 2 ou mais participantes

Fornece funcionalidades que podem servir para implementar:

-Users location

-Users availability

-Negociações de parametros de participação dos utilizadores na sessão

-mecanismos de segurança (Users authentication, Prevent denial of service attacks)…

**SIP functionalities**

-Localização do user por endereço e-mail

-Capacidades do user

-disponibilidade do user

-estabilidade da chamada

-Controlo de chamada

**H.323**

Protocolo para comunicações multimedia

-Pode ser usado por qq IP

-Regras(signaling,control,transport)

-Define tudo, a partir de codecs de uma camara remota

**H.323 protocol stack**

Q391 – call signalling

H245 – criação de canais

RAS, H225 – User registration

Codecs – Audio(G.711) Video(H.261,H.263)

Data – T.12x

Vantagens

-Funciona

-Muitas implementações

-Suporta varias linguagens

-Opera com outras linguagens: H320, H324...

Desvantagens

-Muito complicado

-Pode causar redundância

-Problemas quando Gatekeeper está sobrecarregado e MCU está cheio

-Dificil de desenvolver firewalls

**SIP vs H.323**

Pedido resposta baseado em texto

Tipos de servidor: registador, proxy, redirect

Define um minimo de perfis e extensões

\_

Sub-protocols:H.245,Q931...

H.323 Gatekeeper

Defines extensivamente as funções

\_

Ambos usam RTP/RTCP sobre UDP/IP

H.323 é considerado “heavy-weight”

**8)Mobile**

Wireless Networks

Personal: PANs -> Bluetooth

Local: LANs -> IEEE 802.11

Regional: WANs -> GSM, UMTS

Worldwide: Sattelite -> Iridium

**Types of connections**

Point-to-point networks

Diffusion networks

Semi-diffusion networks

**Mobility agents**

2 entidades

Local mobility agent

-Identifica qual o terminal que não está na rede local

Remote mobility agent

-Identifica o novo terminal que chegou à rede

-encaminha o trafego para o terminal

**Handover**

Transfere o fluxo de informação entre pontos de acesso

Algumas classificações:

-Scope

-Technology

-Connectivity

-Perfomance

**Handover in terms of scope**

Layer 2

Intra-cell

Inter-cell

Inter-network

**Handover in terms of technology**

Intra-technology

Inter-technology

Horizontal

Vertical

**in terms of connectivity**

Make-before-break handover(soft)

Break-before-make handover(hard)

**In terms of performance**

Smooth handover

Fast handover

Seamless handover

Context-aware handover

**Cells**

Vantagens

>capacidade

>#users

<power

>robustness (distributed system)

Desvantagens

-Rede cablada entre telefones

-Many handovers

-Interferência

Fundamental

-Dimensão

\_tamanho

\_reserva de canais