Tipos de Encaminhamento

O **encaminhamento estático** é predefinido por configuração estática. Define-se o next-hop para atingir uma determinada rede; O next-hop deverá ser o endereço do próximo router do caminho e deverá pertencer a uma rede que o router já conheça; É necessário a definição de uma rota estática para cada rede para a qual se pretende conectividade (pode-se usar 0.0.0.0/0 que representa todas as redes -> Rotas por Omissão)

O **encaminhamento dinâmico** pressupõe o uso de um protocolo de comunicação entre nós da rede de modo a determinar as redes existentes e os melhores caminhos (next-hops) para as atingir. O encaminhamento dinâmico é preferível, no entanto, em cenários simples o encaminhamento estático pode ser aceitável.

- O encaminhamento dinâmico permite à rede adaptar-se automaticamente a mudanças na topologia, sem envolvimento do administrador. Quando a topologia da rede muda, a nova informação é dinamicamente propagada pela rede, e cada router atualiza a sua tabela de encaminhamento de modo a refletir as alterações.

RIP

RIP v1	RIP v2
É um protocolo classful - Não anuncia as sub-máscaras das redes -	É um protocolo classless - Os anuncios RIPv2 incluem o prefixo e a sub-máscara de rede - Suporta máscaras de tamanho variável
RIPv1 usa o endereço 255.255.255.255 para enviar os seus anúncios - Todos os equipamentos, incluindo PC e servidores, têm de processar os pacotes	RIPv2 usa o endereço 224.0.0.9 para enviar os seus anúncios apenas para os routers a correr no protocolo RIPv2.
Não suporta autenticação de mensagens	RIPv2 suporta autenticação de mensagens usando message-digest ou autenticação em texto aberto.

Pacotes trocados entre Routers - RIP Request e RIP Response.

OSPF

Eleição do Designated Router (DR) e Backup Designated Router (BDR) - Os routers OSPF em redes broadcast (como LAN Ethernet), elegem um Router com Designated Router (DR) e outro como Backup Designated Router (BDR), no qual todos os routers formam adjacências com estes dois routers. O primeiro router a ser ligado torna-se o DR e o segundo o BDR. Caso vários routers arranquem em simultâneo, o DR será o router que, de entre os ligados à LAN, tiver maior prioridade. Em caso de empate será escolhido o router com maior router ID. Após um router ser eleito DR, nenhum outro router poderá ser. Se o DR avariar, o BDR será o novo DR e será eleito um novo BDR.

Tipo de pacotes OSPF

Hello: Para descoberta de vizinhos, construção de adjacências com eles e eleição do DR e BDR. Não transporta informação de encaminhamento; a sua receção não altera as base dados pelo que não requer processamento das tabelas de encaminhamento.
Database Description (DBD): Usado para a verificação do conteúdo e sincronização das base dados.
Link-State Request (LSR): Usado para pedir um Link-State Advertisement (LSA).
Link-State Update (LSU): Usado para enviar os Link-State Advertisement (LSA).
LSAck: Confirma a correta correção dos pacotes.

RIP	OSPF
Protocolo mais simples	Protocolo complexo (para sincronizar base de dados distribuídas)
Encaminhamento baseado em n' de saltos	Escalável (para grandes redes, a solução é o encaminhamento hierárquico)
Não é escalável (finito=16)	Maior flexibilidade de encaminhamento (baseado em custos configuráveis)
Processamento continuo de tabelas de encaminhamento	Processamento pontual das tabelas de encaminhamento
	Utilização intensa da rede apenas quando há alterações da topologia da rede (processo de flooding)
	Processo de convergência das tabelas de encaminhamento mais rápido

BGP

Tipo de pacotes BGP

Open: Começam por estabelecer relações de vizinhança (ex: declarar o nº de SA); inicialmente são trocadas todas as rotas BGP
Update: Transporta informações de encaminhamento
KeepAlive: Na hipótese de não haver alterações de rotas, são enviadas periodicamente entre vizinhos para relações de vizinhança.
Notification: Transmitidos para reportar situações de erro e terminar relações.

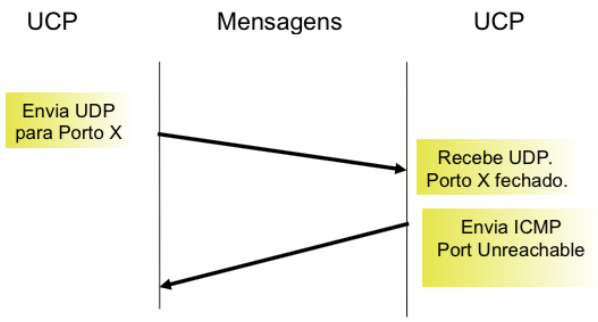
Seleção de Caminhos BGP

O BGP pode receber múltiplos anúncios para uma mesma rota a partir de múltiplas fontes. O BGP seleciona apenas um caminho como o melhor. O BGP coloca o caminho selecionado na tabela de encaminhamento de IP e propaga-o aos seus vizinhos.

UDP - User Datagram Protocol

Proporciona um serviço de transporte de dados com as características de desempenho oferecidas pela rede IP. Permite a troca de dados entre aplicações, e não apenas entre estações, através de introdução no seu cabeçalho de um campo identificador do porto. Permite o envio de dados para múltiplos destinos

Porto UDP Fechado

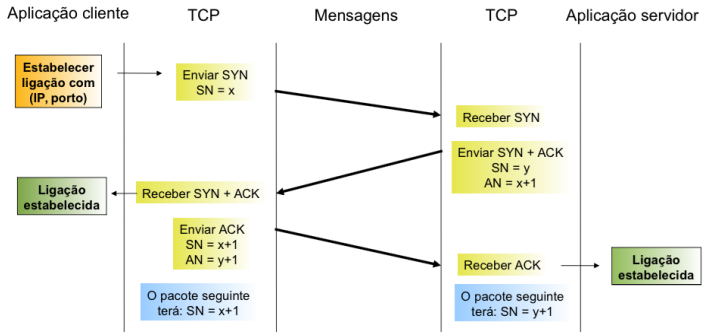


TCP - Transmission Control Protocol

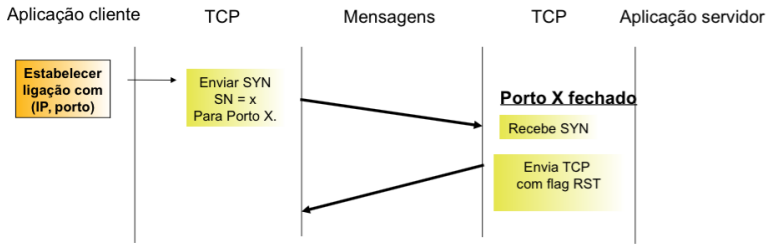
• Proporciona um serviço de transporte de dados fiável
  - os dados são recebidos pela aplicação destino sem falhas e pela ordem enviada
• É orientado à ligação
  - as estações estabelecem um canal lógico ao qual são atribuídos os identificadores das aplicações, bem como os recursos de memória necessários para que os dados sejam transmitidos de uma forma fiável
• É bi-direccional
  - são estabelecidos dois canais lógicos independentes, um em cada sentido
• Suporta apenas ligações ponto-a-ponto
• Faz uso da noção de fluxo de informação
  - o emissor secciona os dados de uma forma independente dos blocos de informação que lhe são entregues para envio pela aplicação origem
• Proporciona o estabelecimento e a terminação da ligação transparente
  - uma aplicação pede para estabelecer uma ligação: se o TCP responder à aplicação com uma mensagem de sucesso, significa que existe conectividade com a estação destino e que a aplicação destino está preparada para comunicar
uma aplicação pede para terminar uma ligação: o TCP assegura que se houver informação ainda por enviar, ela é transmitida antes de sinalizar a terminação da ligação

Formato de um segmento TCP
URG - Campo Urgent Pointer válido
ACK - Campo Acknowledgment válido
PSH - Os dados requerem um push
RST - Fazer reset à ligação
SYN - Sincronizar sequence number
FIN - Origem terminou o envio da informação

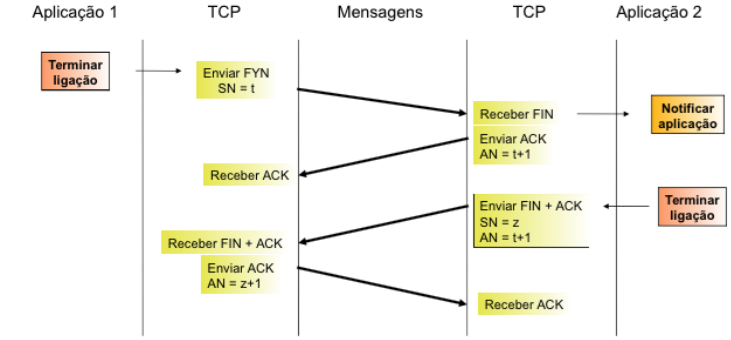
Estabelecimento de uma ligação TCP



Tentativa de estabelecimento de uma sessão para um porto fechado



Terminação de ligação em TCP



NAT e PAT

Este mecanismo faz a tradução de endereços privados em públicos com diferenciação por porto aquando o acesso ao exterior da rede. O NAT/PAT irá alterar os endereços no cabeçalhos IP (e se necessário nos cabeçalhos das camadas superiores), guardar a relação endereço/porto privado com endereço/porto público de modo a restaurar os endereços privados aquando da resposta do exterior.

Segurança

Firewall - Sistema ou grupo de sistemas que impõe uma política de controlo entre duas ou mais redes. Uma firewall é um sistema de filtragem de pacotes (Encaminha pacotes entre os hosts internos e externos, de forma seletiva) impedindo acessos.
Limitações: Ineficazes contra ataques internos ou ataques de maquinas comprometidas; só consegue controlar o tráfego aberto no ponto de entrada da rede; difícil de gerir em rede com interesses e necessidades heterogéneas(ex:universidades).

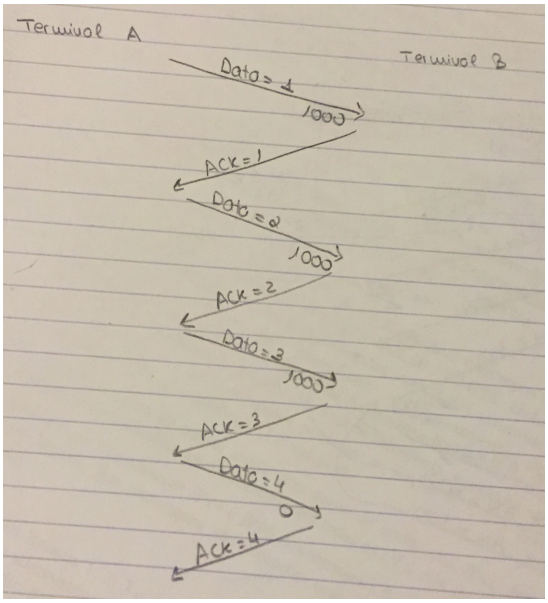
ACL - Utilizado na filtragem de tráfego e controlar quem pode aceder a quê e onde.
Tipos de ACL
Standard - Controlo de tráfego através da análise de endereço de origem dos pacotes IP.
Extended - Controlo de tráfego através da análise dos endereços de origem e de destino e protocolos dos pacotes IP.
Named - Permite aos ACL Standard e Extended que recebem nomes em vez de números.
Reflexive - Permite que os pacotes IP sejam filtrados com base nas informações da sessão da camada superior. A comunicação num sentido abre portas no sentido oposto. Geralmente usado para permitir o tráfego de saída e limitar o tráfego de entrada, em resposta a sessões que se originam dentro da rede.

Túnel IPSec - Garante a confidencialidade da transmissão e integridade dos dados (na camada de rede) entre duas redes distintas, fornece encriptação de dados (os dados não vão em "texto aberto").

VPN - Conexão criptografada entre redes privadas através de uma rede pública. Garante a confidencialidade da transmissão e integridade dos dados (na camada de rede) entre duas redes distintas, fornece encriptação de dados (os dados não vão em "texto aberto").

Aplicações Cliente - Servidor

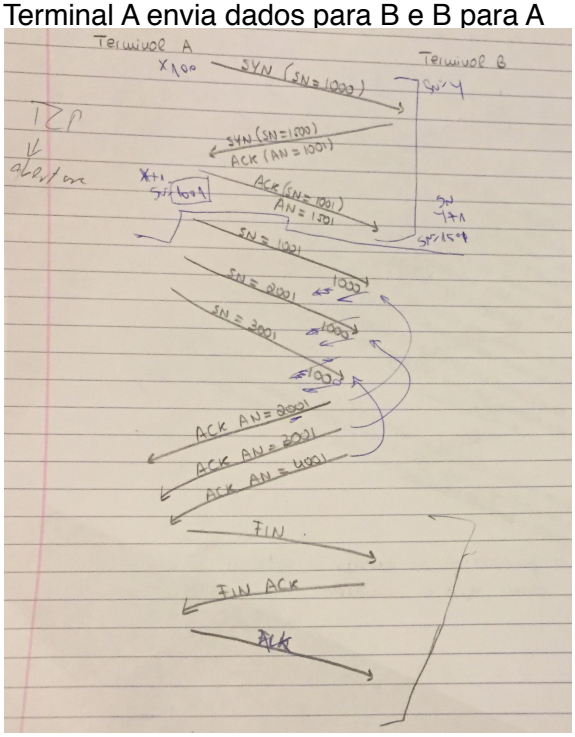
TFTP
Terminal A envia dados (3000bytes, 1000 cada vez) para Terminal B



A envia os dados (1000bytes de cada vez) para B e B responde com mensagens ACK a receção dos dados. O Terminal B cria o ficheiro de dados quando o último pacote enviado tiver um tamanho menor ao imposto(neste caso 1000bytes)

TCP

Terminal A envia dados para B e B para A



O uso do protocolo TPC implica a abertura (SYN) e fecho da sessão (FIN).
Após a abertura, o resultado do SN = SN+1 e ACK = ACK + 1

FTP

• Serviço de transferência de ficheiros

• Corre sobre TCP e o servidor usa dois números de porto. Ligação de controle: porto 21 Ligação de dados: porto 20

• Possui mecanismos de autenticação Username + Password ou Username Anonymous (Credenciais são transmitidas em texto aberto)

• Numa sessão FTP:

O cliente estabelece uma ligação de controlo com o servidor por onde são trocados os comandos FTP; A ligação de controle mantém-se activa até terminar a sessão FTP; Sempre que é necessário uma transferência de dados, o servidor estabelece uma ligação de dados do seu número de porto 20 para um número de porto previamente anunciado pelo cliente pelo comando PORT ; No fim da transferência de dados, o servidor termina a ligação de dados

HTTP

• O HTTP inclui um processo de autenticação que permite limitar o acesso a ficheiros com base num username e password.

• Uma mensagem request enviada por um browser para um ficheiro protegido é respondida pelo servidor com uma mensagem response em que a linha de resposta é: 401 Authorization Required

• Esta resposta inclui uma linha de cabeçalho do tipo WWW-Autenticate indicando o método de autenticação a usar

• O novo pedido inclui uma linha de cabeçalho do tipo Authorization com a informação do username e password gerada pelo método pedido pelo servidor

• Tipicamente, o browser guarda a informação de username e password em memória para ser usada em futuras mensagens de request

Cookies - Os cookies são uma forma do servidor identificar um terminal em diferentes pedidos feitos no tempo. Permite ao servidor diferenciar a informação a disponibilizar por terminal
A primeira vez que um terminal enviar um request a um servidor, o servidor inclui na resposta uma linha de cabeçalho. Se o browser for configurado para aceitar cookies, ele guarda este número juntamente com o identificador do servidor.

Proxy - Os servidores proxy nas empresas ou instituições:
•Diminuem os tempos de interação
•Reduzem o tráfego para a rede pública
•Os servidores proxy nas redes dos Internet Service Providers (ISPs):
•Permitem uma infra-estrutura de distribuição automática dos conteúdos Web mais solicitados por elementos de rede que estão topologicamente perto dos clientes

Correio Electrónico

Envio de mensagens de correio electrónico (entre mail servers):
• SMTP (Simple Mail Transfer Protocol)
Envio de mensagens de correio electrónico (do user agent para o mail server do emissor)
•SMTP (Simple Mail Transfer Protocol), HTTP (Hyper-Text Transport Protocol)
Acesso à caixa de correio electrónico (envio do mail server para o user agent)
•POP3 (Post Office Protocol – versão 3), IMAP (Internet Mail Access Protocol), HTTP (Hyper-Text Transport Protocol)

SMTP	POP3	IMAP
- A comunicação é estabelecida pela entidade que pretende enviar informação(push protocol) - Comunicações diretas: por omissão, o mail server do emissor envias as mensagens diretamente para o mail server dos receptores.	- A comunicação é estabelecida pela entidade que pretende receber informação(pull protocol) - A transferência de mensagens é feita de dois modos: 1) Envio e remoção: as mensagens são removidas da caixa correio após envio. 2) Envio e armazenamento: as mensagens são mantidas na caixa correio após envio.	Relativamente ao POP3, o IMAP permite ao utilizador funcionalidade adicionais importantes: - criar e gerir um sistema de directórios de mensagens no servidor; fazer operações de procura no sistema de directórios(útil para utilizadores que usem o serviço de múltiplos terminais) - solicitar o envio de partes das mensagens de correio(útil quando o terminal está ligado à rede através de ligações de baixo débito)

Multicast

IGMP - Serve para os terminais anunciarem aos routers a intenção de participação/desistência de uma sessão multicast.
Mensagens IGMP
• **GMQ - General Membership Query -** Enviado pelos routers para perguntar se as estações participam em alguma sessão multicast
• **SMQ - Specific Membership Query -** Enviado pelos routers para perguntar se existe alguma estação que participe numa sessão multicast específica
• **MR - Membership Report -** Enviado pelas estações para sinalizarem que participam numa sessão multicast
• **LGR - Leave Group Report (Opcional) -** Enviado pelas estações para sinalizarem que deixam de participar numa sessão multicast

Em cada rede, o Querier Router é o router que tiver menor endereço IP na interface ligada à rede e é aquele que mantém o "diálogo" IGMP com os terminais.

Qualquer estação pode juntar-se a uma sessão multicast recendo e enviando informação. A formação de sessões multicast é iniciada pelos receptores(os emissores não controlam que estações podem receber informação). A rede não providencia filtragem, ordenação ou privacidade dos pacotes multicast.

PIM Dense Mode - Utilizado em situações em que os membros de um determinado grupo se encontram distribuídos por toda a rede e abrange assim grande parte dos routers da rede a participarem no processo de routing do datagram multicast.
O PIM Dense Mode utiliza a técnica de "flood and prune". Inicialmente os pacotes multicast são enviados para toda a rede e depois são "cortados" todos os ramos da rede que não tenham terminais interessados nessa informação. Isto é: Manda para todas as redes pacotes mulitas mas quem quer adere ou outros são cortados.

PIM Sparse Mode - Aqui o número de routers com utilizadores multicast é pequeno comparativamente ao número de routers da rede, especialmente quando lidamos com grandes quantidades de tráfego comparativamente à largura de banda. Quando um router (DR) recebe datagramas de um terminal para ser distribuído pela rede, este encapsula em mensagem PIM de controlo e reencaminhamento unicast para o "Rendezvous Point" (RP). O RP é responsável pela distribuição das mensagens para os destinos pretendidos. Isto é: Quando abre a uma sessão multicast o equipamento que adere pede para receber pacotes multicast.
Adesão à Group-Shared Tree - Os routers recetores enviam uma mensagem join em direção do RP de modo a se juntarem à grous-shared tree que tem a sua raiz no rendezvous point.

P2P

Peer-to-Peer Systems: sistemas distrivuidos que operam sem uma organização centralizada ou qualquer tipo de controlo
Overlay Networks: permitem criar topologias estruturadas virtuais sobre protocolos de transporte básicos, facilitando pesquisas determinística e garantindo convergencia
Pure P2P: referem-se a ambientes onde todos os nós participativos são peers onde não existem sistemas centrais de controlo existindo facilidades para o intercambio entre peers
Hybrid P2P: referem-se a ambientes onde os servidores precisam de activar os peers quando estes querem interagir entre si
O grau do envolvimento do sistema varia consoante a aplicação
Uma rede **P2P não Estruturada** não é composta por uma estrutura lógica e determinística para organizar e gerir os nós peers uma vez que não há um conhecimento prévio da topologia.
Numa rede **P2P Estruturada** a gestão dos peers é feita com uma estrutura lógica e determinista implícita, onde toda a topologia é controlada na íntegra.