



Fundamentos de Redes de Computadores

Prof.: MSc. Alex Junior Nunes

alex.nunes@unicesumar.edu.br

IPv6

- IPv6 é a versão mais atual do Protocolo de Internet
- Originalmente oficializada em 6 de junho de 2012, é fruto do esforço do IETF para criar a "nova geração do IP" (IPng: Internet Protocol next generation), cujas linhas mestras foram descritas por Scott Bradner e Allison Marken, em 1994, na RFC 1752
- Sua principal especificação encontra-se na RFC 2460
- O protocolo está sendo implantado gradativamente na Internet e deve funcionar lado a lado com o IPv4, numa situação tecnicamente chamada de "pilha dupla" ou "dual stack", por algum tempo

IPv6

- A longo prazo, o IPv6 tem como objetivo substituir o IPv4, que suporta somente cerca de 4 bilhões^(escala curta)/mil milhões^(escala longa) (4×10^9) de endereços IP, contra cerca de 340 undecilhões^(escala curta)/sextilhões^(escala longa) ($3,4 \times 10^{38}$) de endereços do novo protocolo
- Um aperfeiçoamento é que o IPv6 utiliza 128 bits para representar seus endereços, contra os 32 bits do IPv4
- Um segundo aperfeiçoamento importante no IPv6 é a simplificação do cabeçalho, sendo que ele contém apenas sete campos (contra os 13 do IPv4)
- Essa mudança permite aos roteadores processar os pacotes com mais rapidez e, dessa forma, melhorar o throughput e o atraso

IPv6

- Os endereços foram ao longo do tempo otimizado, para que nos casos onde haja a presença de 0, esses possam ser omitidos
- Endereço completo
- 8000:0000:0000:0000:0123:4567:89AB:CDEF
- Endereço novo (otimizado)
- 8000::123:4567:89AB:CDEF

Comparação

IPv4

Implantado em 1981

Endereço IP de 32-bit

4,3 bilhões de endereços

Endereços precisam ser reutilizados e mascarados

Notação numérica decimal com ponto

192.168.5.18

DHCP ou configuração manual

IPv6

Implantado em 1998

Endereço IP de 128-bit

340 undecilhões de endereços

Cada dispositivo tem um endereço exclusivo

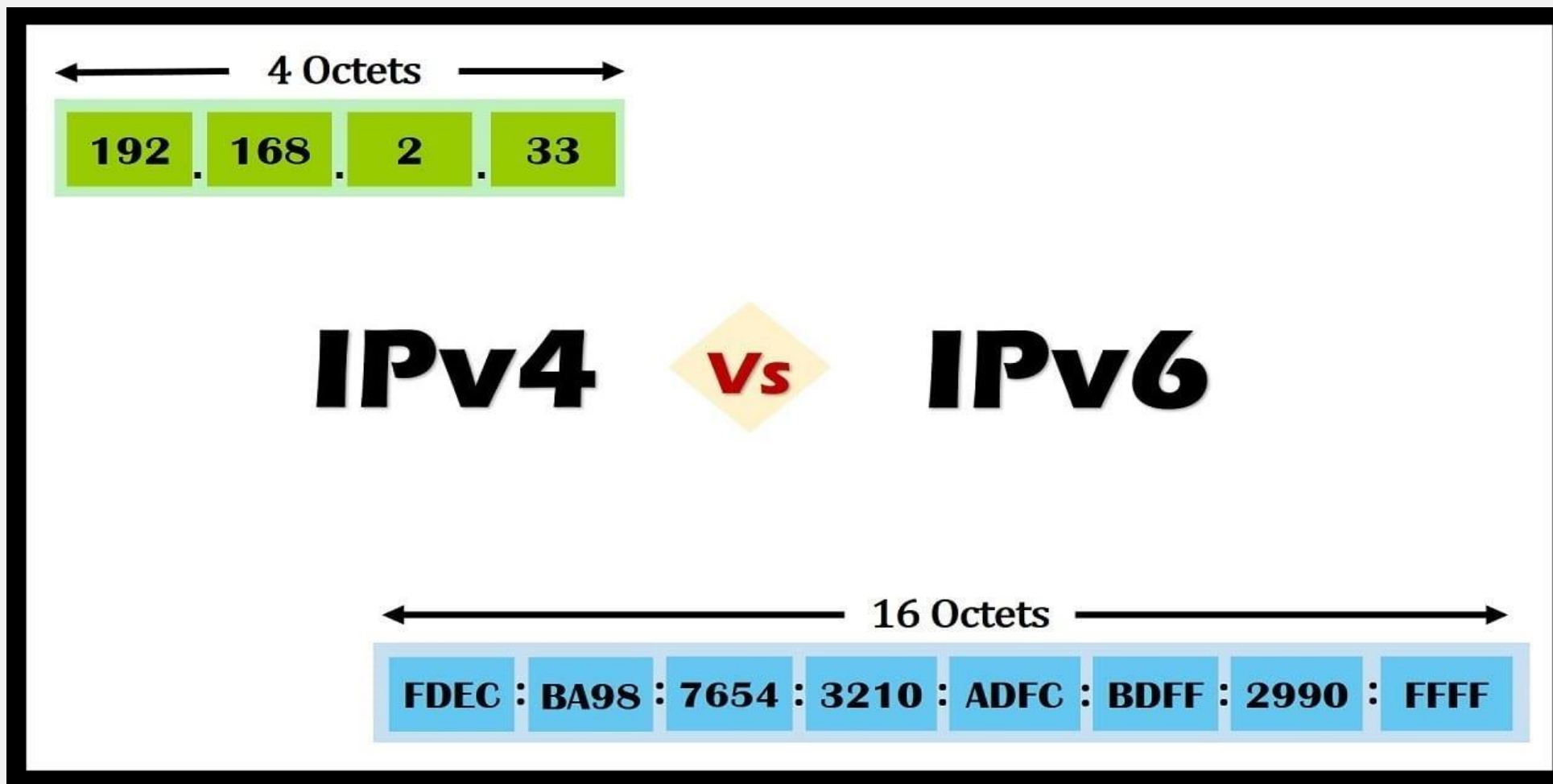
Notação hexadecimal alfanumérica

50b2:6400:0000:0000:6c3a:b17d:0000:10a9

(Simplificado - 50b2:6400::6c3a:b17d:0:10a9)

Compatível com configuração automática

Comparação



Traceroute

- **Traceroute** é uma ferramenta de diagnóstico que rastreia a rota de um pacote através de uma rede de computadores
- Ele utiliza os protocolos IP e o ICMP, implementada pela primeira vez por Van Jacobson em 1988
- Atualmente está disponível em diversos sistemas operacionais como Linux, FreeBSD, NetBSD, MacOS X e Windows
- Seu funcionamento está baseado no uso do campo Time to Live (TTL) do pacote IPv4 destinado a limitar o tempo de vida dele
- Este valor é decrementado a cada vez que o pacote é encaminhado por um roteador

Traceroute

- Ao atingir o valor zero o pacote é descartado e o originador é alertado por uma mensagem ICMP TIME_EXCEEDED
- Através da manipulação do campo TTL de uma série de datagramas UDP é possível receber esta mensagem de cada um dos roteadores no caminho do pacote
- Para o caso do IPv6 é utilizado o campo hop limit, o limite de saltos dos datagramas desta versão do protocolo
- A implementação disponível no Microsoft Windows utiliza apenas pacotes ICMP

Traceroute

- O traceroute pode ser limitado (quantidade de saltos), pois um rastreamento pode ter muitos saltos
- Para executar o Traceroute dentro do Windows basta digitar no CMD o comando `tracert` + o endereço desejado
- `tracert google.com`

Outros protocolos

DHCP

- DHCP é sigla para Dynamic Host Configuration Protocol (protocolo de configuração dinâmica de host)
- É um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host, máscara de sub-rede, default gateway (gateway padrão), número IP de um ou mais servidores DNS, sufixos de pesquisa do DNS e número IP de um ou mais servidores WINS
- Este protocolo é o sucessor do BOOTP que, embora mais simples, tornou-se limitado para as exigências atuais. O DHCP surgiu como um padrão em outubro de 1993
- O RFC 2131 (1997) contém as especificações mais atuais. O último standard para a especificação do DHCP sobre IPv6 (DHCPv6) foi publicado como RFC 3315 (2003)

DHCP

- O DHCP usa um modelo cliente-servidor
- Resumidamente, o DHCP opera da seguinte forma:
 - Quando um computador (ou outro dispositivo) se conecta a uma rede, o host/cliente DHCP envia um pacote UDP em broadcast (destinado a todas as máquinas) com uma requisição DHCP (para a porta 67);
 - Qualquer servidor DHCP na rede pode responder a requisição. O servidor DHCP mantém o gerenciamento centralizado dos endereços IP usados na rede e informações sobre os parâmetros de configuração dos clientes como gateway padrão, nome do domínio, servidor de nomes e servidor de horário
 - Os servidores DHCP que capturarem este pacote responderão (se o cliente se enquadrar numa série de critérios) para a porta 68 do host solicitante com um pacote com configurações onde constará, pelo menos, um endereço IP e uma máscara de rede, além de dados opcionais, como o gateway, servidores de DNS, etc



TCP

- Protocolo de Controle de Transmissão
- Transmission Control Protocol (TCP)
- É um dos protocolos de comunicação, da camada de transporte da rede de computadores do Modelo OSI, que dão suporte a rede global Internet, verificando se os dados são enviados na **sequência correta** e **sem erros** via rede
- É complementado pelo protocolo da Internet, normalmente chamado de, TCP/IP



TCP

- Neste protocolo da camada de transporte (camada 4 OSI) se assentam a maioria das aplicações cibernéticas, como o SSH, FTP, HTTP — portanto, a World Wide Web, devido sua versatilidade e robustez
- O Protocolo de controle de transmissão provê confiabilidade, entrega na sequência correta e verificação de erros dos pacotes de dados, entre os diferentes nós da rede, para a camada de aplicação
- Aplicações que não requerem um serviço de confiabilidade de entrega de pacotes podem se utilizar de protocolos mais simples como o User Datagram Protocol (UDP), que provê um serviço que enfatiza a redução de latência da conexão



UDP

- O User Datagram Protocol (UDP) é um protocolo simples da camada de transporte
- Ele é descrito na RFC 768 e permite que a aplicação envie um datagrama encapsulado num pacote IPv4 ou IPv6 a um destino, porém **sem qualquer tipo de garantia** que o pacote chegue corretamente (ou de qualquer modo)
- O protocolo UDP não é confiável
- Caso garantias sejam necessárias, é preciso implementar uma série de estruturas de controle, tais como timeouts, retransmissões, *acknowledgements*, controle de fluxo, etc



UDP

- Cada datagrama UDP tem um tamanho e pode ser considerado como um registro indivisível, diferentemente do TCP, que é um protocolo orientado a fluxos de bytes sem início e sem fim
- Também dizemos que o UDP é um serviço sem conexão, pois não há necessidade de manter um relacionamento longo entre cliente e o servidor
- Assim, um cliente UDP pode criar um socket, enviar um datagrama para um servidor e imediatamente enviar outro datagrama com o mesmo socket para um servidor diferente



UDP

- Da mesma forma, um servidor poderia ler datagramas vindos de diversos clientes, usando um único socket
- O UDP também fornece os serviços de broadcast e multicast, permitindo que um único cliente envie pacotes para vários outros na rede



UDP

- Em comparação ao TCP, é possível entendê-lo como um envio de cartas pelo correio:
- Onde o usuário escreve a carta, envelope como o endereço de origem e destino, envia, mas não consegue ter a confirmação imediata se aquilo chegou ou não ao destino, ele só tem certeza do envio
- Já o TCP pode ser tido como um telefone, onde é possível saber de imediato se o destinatário está ou não recebendo as informações

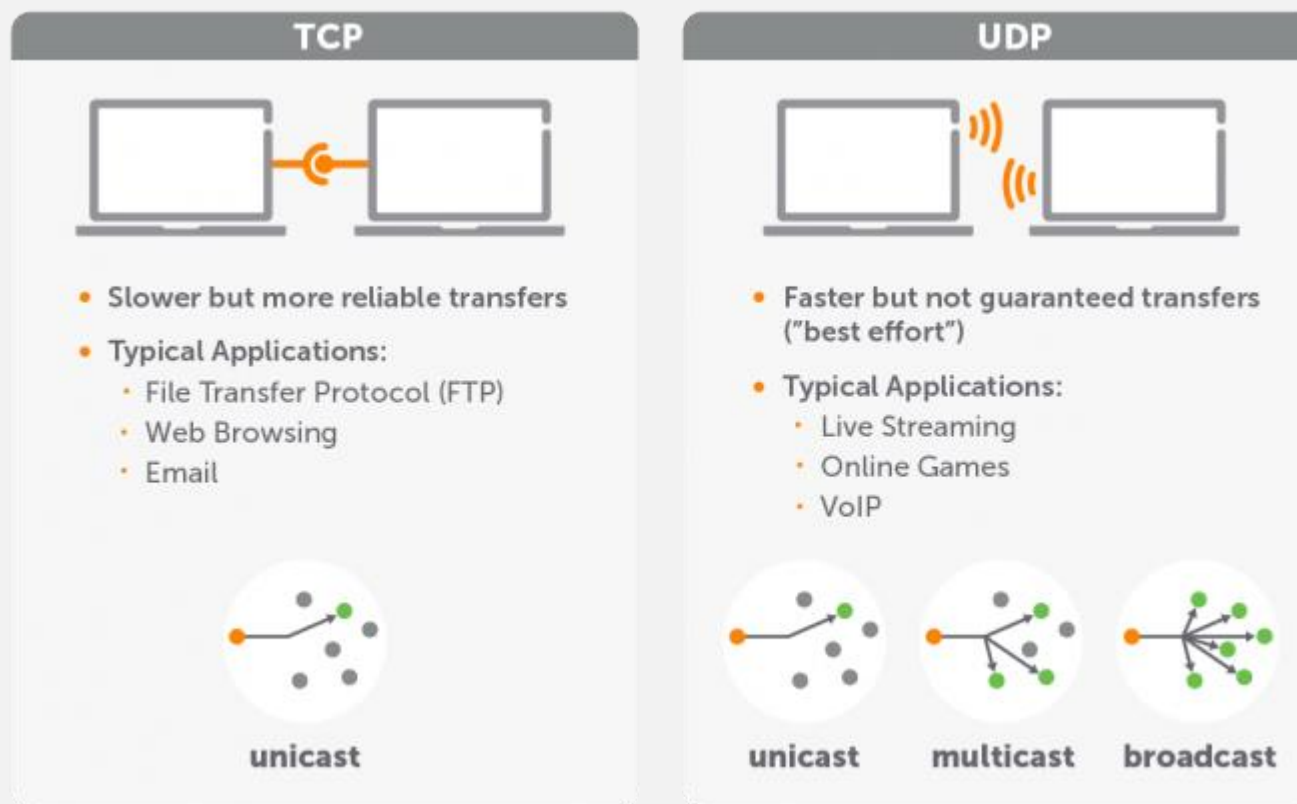
TCP x UDP

TCP	UDP
Keeps track of lost packets. Makes sure that lost packets are re-sent	Doesn't keep track of lost packets
Adds sequence numbers to packets and reorders any packets that arrive in the wrong order	Doesn't care about packet arrival order
Slower, because of all added additional functionality	Faster, because it lacks any extra features
Requires more computer resources, because the OS needs to keep track of ongoing communication sessions and manage them on a much deeper level	Requires less computer resources
Examples of programs and services that use TCP: <ul style="list-style-type: none"> - HTTP - HTTPS - FTP - Many computer games 	Examples of programs and services that use UDP: <ul style="list-style-type: none"> - DNS - IP telephony - DHCP - Many computer games

TCP x UDP

TCP	UDP
Secure	Unsecure
Connection-Oriented	Connectionless
Slow	Fast
Guaranteed transmission	No Guarantee
Used by critical applications	Used by real-time applications
Packet reorder mechanism	No reorder mechanism
Flow control	No flow control
Error Checking	No Error Checkin
20 Bytes Header	8 Bytes Header
Acknowledgement Mechanism	No Acknowledgement
Three-way handshake (SYN, SYN-ACK, ACK)	No handshake
DNS, HTTP, HTTPS, FTP, SMTP, Telnet, SNMP	DNS, DHCP, TFTP, SNMP, RIP, VOIP

TCP x UDP





DNS

- Sistema de Nomes de Domínio
- Em inglês Domain Name System (DNS)
- É um sistema hierárquico e distribuído de gestão de nomes para computadores, serviços ou qualquer máquina conectada à Internet ou a uma rede privada
- Ele faz a associação entre várias informações atribuídas a nomes de domínios e cada entidade participante
- A sua utilização mais convencional associa nomes de domínios mais facilmente memorizáveis a endereços IP numéricos, necessários à localização e identificação de serviços e dispositivos, processo esse denominado por: resolução de nome



DNS

- O desempenho não se degrada substancialmente quando se adicionam mais servidores
- Por padrão, o DNS usa o protocolo User Datagram Protocol (UDP) na porta 53 para servir as solicitações e as requisições
- O DNS apresenta uma arquitetura cliente/servidor, podendo envolver vários servidores DNS na resposta a uma consulta
- O servidor DNS resolve nomes para os endereços IP e de endereços IP para os nomes respectivos, permitindo a localização de hosts num determinado domínio



DNS

- Existem centenas de servidores-raiz DNS (root servers) no mundo todo, agrupados em 13 zonas DNS raiz, das quais sem elas a Internet não funcionaria
- Destes, dez estão localizados nos Estados Unidos da América, dois na Europa e um na Ásia
- Para aumentar a base instalada destes servidores foram criadas réplicas localizadas por todo o mundo, inclusive no Brasil desde 2003