

Redes de Computadores I

Aula 06 - Arquitetura Internet – Parte III

Apresentação

Na aula anterior você viu como se dá o funcionamento do protocolo fundamental para o funcionamento da Internet: o protocolo IP. Nesta aula explicaremos outros fundamentos e protocolos também relacionados a camada de rede da arquitetura TCP/IP, tais como roteamento, o ICMP e a nova versão do protocolo IP, conhecida como IPv6.

Objetivos

- Definir configurações IP em um host.
- Entender superficialmente o que é roteamento.
- Conhecer o protocolo ICMP.
- Introduzir superficialmente o protocolo IPv6.

ICMP – Protocolo de Mensagens de Controle da Internet

A camada de Rede, do modelo TCP/IP, que é utilizado na prática da Internet, é composta basicamente de três componentes: o protocolo IP, os protocolos de roteamento (veremos os princípios nesta aula e nos aprofundaremos em aulas posteriores) e o ICMP, que estudaremos agora.

O ICMP (Internet Control Message Protocol), ou protocolo de mensagem de controle da Internet, é utilizado pelos hosts e roteadores da rede e servem para reportar informações da camada de rede entre eles, sendo também utilizado para realizar testes na rede. A maior utilização do ICMP é para reportar erros de comunicação. Um exemplo clássico do uso desse protocolo é quando estamos tentando acessar um servidor FTP ou mesmo um servidor web e recebemos uma mensagem que a rede de destino está inalcançável, ou que foi esgotado o tempo limite do pedido, dentre outras. Todas essas mensagens são originadas pelo ICMP. O fato de a rede estar indisponível se deve à falha em algum lugar, entre a origem e o destino, e assim o último roteador que recebeu o pacote e não conseguiu entregar ao próximo roteador emite uma mensagem ao host remetente explicando que dali para frente existe algum problema que impede que ele entregue o pacote ao destinatário.



Vídeo 01 - Internet

Existem cerca de 12 tipos de mensagens ICMP definidas que são transportadas dentro de pacotes IPs. As mensagens ICMP têm alguns campos e dentre eles estão os campos Tipo e campo Código. O Quadro 1 apresenta os principais tipos de mensagens ICMP.

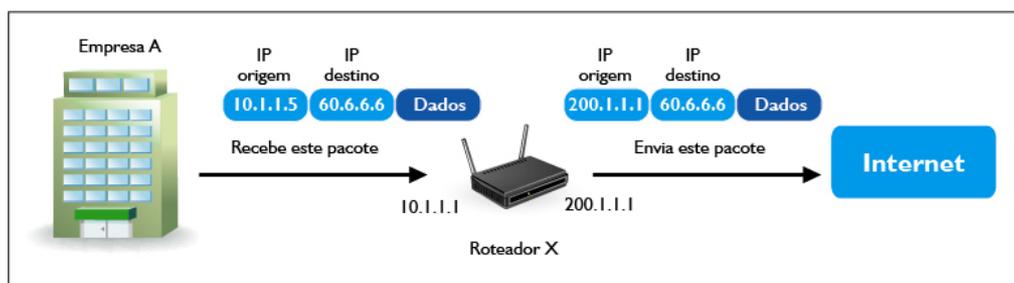
Tipo de mensagem ICMP	Código	Descrição
0	0	Resposta de eco do ping
3	0	A rede não está acessível
3	6	Rede de destino desconhecida
3	3	Porta não disponível
10	0	Descoberta do roteador
9	0	Anúncio do roteador

Quadro 1 - Tipos de mensagens ICMP

Dentre as mensagens mais comuns, podemos mencionar as mensagens ECHO e ECHO REPLY, que são enviadas pelos hosts para ver se outro host destino pode ser alcançado e está ativo. Para vermos na prática as respostas das mensagens ICMP, vamos fazer um teste com o comando ping. Você deve se orientar pelos seguintes passos em sua máquina rodando uma versão do Sistema Operacional Windows:

1. Clicar no botão Iniciar, depois em Executar e na caixa que aparece digitar cmd (comando que abrirá uma tela preta, que é prompt de comando do Windows – local onde você poderá executar comandos).
2. Uma vez no prompt (tela preta), digite o comando ping www.ufrn.br e você deverá obter uma tela semelhante a da Figura 1

Figura 01 - Resposta do comando ping



Fonte: Autoria própria.

Atividade 01

1. Faça uma pesquisa sobre outros comandos que podemos usar para testar a funcionalidade da rede (ping, net, ipconfig, netstat, net). Use os seguintes endereços como ponto de partida:

- <http://pt.kioskea.net/faq/1319-comandos-ip-relativos-a-redes-no-windows>
- <http://bobdicas.blogspot.com/2007/10/comandos-de-rede-mais-utilizados.html>

Resposta

Resposta

1. Os seguinte comandos são bastante utilizados para testes e gerenciamento das redes. *ipconfig* (Windows) - Fornece informações completas sobre os números ips fornecidos a(s) placas de rede, por Dial-Up e por placa de comunicação. Sintaxe: *ipconfig /all* (mais comum);
netstat (Windows e Linux) - Mostra conexões da rede que estão estabelecidas, qual protocolo está usando, as portas que estão disponíveis para conexão, o endereço local e o endereço externo da conexão, etc. É um status da relativamente completo. Sintaxe: *netstate [opções]*
ping - Envia pacotes ICMP para um host afim de obter uma resposta para saber se o mesmo encontra-se ativo. Sintaxe: *ping endereço_IP* ou *nome*. Ex: *ping www.uol.com.br* *ping 200.19.160.21*.
net - O comando *net* apresenta várias opções de serviço que podem ser usados, para testar a rede e modificar parâmetros:
NET ACCOUNTS NET HELPMMSG NET STATISTICS NET COMPUTER NET LOCALGROUP NET STOP NET CONFIG NET PAUSE ET TIME NET CONTINUE NET SESSION NET USE NET FILE NET SHARE NET USER NET GROUP NET START NET VIEW NET HELP

Configuração IP de uma Máquina

Para que uma máquina funcione em uma rede TCP/IP, ela precisa ter a pilha de protocolos instalada (isso inclui os protocolos ARP, IP, ICMP, TCP e UDP). Normalmente, isso é feito quando se instala o Sistema Operacional. Os protocolos de aplicação não são obrigatórios e devem ser instalados os que se pretende utilizar. Evidentemente, não basta ter o software instalado, algumas coisas precisam ser configuradas para que a máquina funcione na rede. Quais parâmetros você acha que precisam ser configurados?

Tudo que precisamos informar para que a máquina consiga enviar pacotes IP para outras máquinas é o seguinte:

- O endereço IP da máquina;
- A máscara de rede;
- A rota padrão, normalmente chamada de gateway;
- Como nós, pessoas, não vamos conseguir lembrar o endereço IP de todas as máquinas que acessamos, existe um serviço de rede que associa nomes (como, por exemplo, <www.imd.ufrn.br>) ao endereço IP da máquina. Estudaremos esse serviço em aulas posteriores, mas agora tudo que você precisa saber é que devemos informar o endereço IP da máquina que realiza essa tarefa de tradução. Esse parâmetro se chama servidor de nomes (ou servidor DNS).

Atividade 02

1. Utilizando o comando `ipconfig`, descubra o endereço IP e a máscara de rede do computador que você está usando no momento. Em seguida, identifique seu endereço de rede.

[Resposta](#)

Resposta

1. Vai depender diretamente da rede em que o usuário se encontra. Por exemplo: IP = 10.0.0.100; mascara = 255.255.255.0 e endereço de rede = 10.0.0.0;

IPv6 – Internet Protocol Versão 6

Na aula anterior, nós estudamos sobre endereçamento IP, e vimos que iríamos nos deter à versão 4 do protocolo IP, conhecido por todos apenas como IPv4, mas não podemos deixar de apresentar a versão 6 do protocolo IP, mais conhecida como IPv6.

No início da década de 1990, o crescimento da Internet era enorme e cada novo host colocado na rede necessitava de mais um IP. A rede crescia muito rapidamente de maneira que os engenheiros do IETF (Internet Engineering Task Force) perceberam que os IPs disponíveis no espaço de endereçamento fornecido pela versão 4 do protocolo IP, que é composta de 32 bits, não iria ser suficiente por muito tempo (estima-se que os últimos endereços IPv4 disponíveis serão atribuídos até o final de 2015). Assim, eles começaram a estudar e a pensar em uma solução para esse problema, e chegaram a conclusão que a única solução de longo prazo era utilizar endereços maiores.

A solução proposta, e aceita, foi o IPv6 (IP versão 6), um projeto para substituir o IPv4. O IPv6 usa endereços de 128 bits, o que eliminou o problema de escassez de endereços no futuro previsível. Porém, diferente do que aconteceu com os diversos padrões ethernet (em que cada padrão novo era compatível com o padrão anterior), o IPv6 é um protocolo da camada de rede que não é compatível com o IPv4. Por causa disso, e por falta de conhecimento do público em geral (pois as empresas e os usuários não sabiam por que eles deveriam usar o IPv6), o IPv6 é utilizado por uma pequena parte da internet, apesar de ser um padrão desde 1998.

Além de aumentar o número de endereços disponíveis, o projeto do IPv6 também resolve alguns outros problema com o IPv4. Dentre os objetivos do projeto IPv6, podemos citar a simplificação do protocolo, oferecer mais segurança, e questões relacionada a qualidade de serviço

O **Quadro 2** mostra o formato do datagrama da versão 6 do protocolo IP.

Versão	Classe de tráfego	Rótulo de fluxo
Compartilhamento de carga útil	Próximo cabeçalho (Hdr)	Limite de saltos
Endereço da Fonte (128 bits)		
Endereço do destino (128 bits)		
Dados		

Quadro 2

A seguir, listamos as principais mudanças ocorridas no IPv6 em relação ao IPv4

- **Capacidade de endereçamento foi expandida:** o tamanho do endereço IPv6 é de 128 bits, enquanto o IPv4 era de apenas 32 bits. Com o novo tamanho, dizem que daria para colocar um IP para cada grão de areia da terra.
- **Cabeçalho aprimorado de 40 bytes:** foram descartados ou se tornaram opcionais alguns campos do IPv4. O tamanho do cabeçalho agora é fixo de 40 bytes, o que torna o processamento dos datagramas IP mais veloz.
- **Rotulação de fluxo e prioridade:** permite rotular fluxos particulares para os quais o remetente requisita um tratamento diferenciado, como um serviço de qualidade diferente do padrão ou ainda um serviço de tempo real, por exemplo.

- **Versão:** nesse campo, vem a versão do protocolo, e deve vir o número 6 representando a sua versão.
- **Classe de tráfego:** tem função semelhante ao campo TOS do IPv4 (visto na Aula 8).
- **Rótulo de fluxo:** é usado para identificar um fluxo de datagramas e é composto de 20 bits.
- **Comprimento da carga útil:** esse campo tem 16 bits e é tratado como um campo sem sinal que fornece o número de bytes do datagrama e vem antes do cabeçalho, cujo tamanho é 40 bytes.
- **Próximo cabeçalho:** identifica o protocolo ao qual o conteúdo do datagrama deve ser entregue. (Semelhante ao IPv4).
- **Limite de saltos:** o valor desse campo é decrementado de um para cada roteador que o datagrama passa pela rede. Se o valor chegar a zero e o pacote não alcançar o destino, ele será descartado.
- **Endereço de fonte e de destino:** fornece os endereços de origem e destino do datagrama.
- **Dados:** parte da carga útil. Quando um datagrama chega ao seu destino, sua carga útil é extraída e repassada para o protocolo que está especificado no campo próximo cabeçalho.

Agora que você sabe que o IPv6 foi criado porque o IPv4 estava se tornando insuficiente e que o IPv6 deverá se tornar o padrão, como será que as coisas funcionarão durante o tempo em que as duas versões coexistirem? Os sistemas que estão preparados para trabalhar com o IPv6 conseguem manipular (enviar, receber e rotear) os datagramas IPv4, mas os sistemas que utilizam IPv4 não conseguem trabalhar com datagramas IPv6.

Atividade 03

1. O que motivou a criação da nova versão do protocolo IP (IPv6)?
2. Diferencie os protocolos IPv4 e IPv6.

Respostas

1. A motivação da criação do protocolo IP – versão 6 (IPv6) foi motivada pelo grande crescimento do número de computadores ligados à internet, fazendo com que em um curto espaço de tempo a quantidade de IPs disponíveis pelo IPv4 acabaria. Desse modo, o IPv6 foi criado, aumentando consideravelmente a quantidade de endereços disponíveis.
2. As principais diferenças entre as duas versões são: o IPv4 permite apenas a ligação de 4 bilhões (4×10^9) de hosts uma vez que os endereços são descritos em números de 32 bits. Já o IPv6, por ter seus endereços descritos em 128 bits, permite $3,4 \times 10^{38}$ hosts. Além disso, o IPv6 resolve outros problemas da versão anterior, como oferecer maior segurança, simplificar o protocolo e endereçar a qualidade de serviço.

Princípios de Roteamento

Agora que você já viu como é a arquitetura da internet, e entendeu que ela nada mais é do que uma interligação de várias redes menores somando-se até atingir níveis globais, aproveitamos para fazer uma pergunta: você sabe quem é o responsável por fazer a interligação dessas redes? Espero que sim, pois já falamos ao longo desta disciplina e também desta aula. É o roteador, que atua na camada de rede do modelo OSI.

Vamos, então, começar a entender, em mais detalhes, como esse processo de encaminhamento dos pacotes ocorre. Você viu na disciplina de Sistemas de Conectividade como as camadas tratam suas PDUs (*Unit Protocol Data* – Unidade de Dados do Protocolo). Lá vimos que em um [host](#). (Qualquer máquina ou computador conectado a uma rede), que está transmitindo, à medida que a informação vem descendo nas camadas, a camada inferior vai encapsulando a PDU que ela recebe da camada superior. Assim, teremos que na camada de rede vão estar os dados que

já foram encapsulados por cada uma das camadas superiores, e esta, por sua vez, acrescenta o cabeçalho IP, gerando a PDU da camada de rede. Essa PDU, que se chama pacote IP, é passada à camada de enlace para ser encapsulada em um quadro (PDU da camada de enlace) e transmitida até o próximo roteador do percurso a ser percorrido até o destino.

Mas, agora surge outra pergunta: como um roteador sabe para qual dos vários roteadores existentes na rede ele deverá enviar o quadro? Em cada roteador existe uma tabela, chamada de tabela de roteamento, que é consultada na hora em que o quadro chega ao roteador, para que seja determinado qual será o próximo roteador, para onde o quadro deverá ser enviado.

Como seria impossível ter uma entrada nessa tabela para cada possível máquina da internet, o esquema de endereçamento IP (que você vai estudar na próxima sessão) agrupa todas as máquinas de uma rede física em uma mesma rede IP, e atribui um endereço a essa rede. Desse modo, as tabelas de roteamento contêm entradas para as redes onde as máquinas estão, ao invés de uma entrada para cada máquina individual. Assim, com apenas uma entrada na tabela, é possível localizar todas as máquinas de uma mesma rede.

Quando um roteador recebe um pacote, ele verifica, em sua tabela de roteamento, a qual das redes o endereço IP de destino do pacote pertence, e encaminha o pacote para o roteador indicado. Esse processo de consulta nas tabelas vai acontecendo roteador a roteador (*hop-by-hop*) até que o quadro chegue ao destino. A **Quadro 3** mostra uma tabela de roteamento simplificada.

Rede de Destino	Próximo Roteador
192.168.100.0	192.168.0.1
200.241.50.0	200.241.48.1

Quadro 3 – Tabela de roteamento

Observe que as informações que são transmitidas são quadros da camada de enlace (transmitidos como bits pelo nível físico). Esses quadros vão sendo passados de roteador para roteador (pode haver vários entre a origem e o destino) até chegar

ao destino. Cada roteador “abre” o quadro e obtém um pacote IP, uma vez que trabalham na camada de rede. Após analisar o pacote IP e consultar sua tabela de roteamento, o roteador coloca o pacote em outro quadro e o envia para o próximo roteador.

Entretanto, temos um problema. A tabela de roteamento identifica o próximo roteador pelo seu endereço IP, mas precisamos do endereço MAC (*Media Access Control* – Controle de Acesso ao Meio) de sua placa de rede para podermos enviar um quadro para ele. Portanto, alguém tem que descobrir o endereço MAC de uma placa a partir do seu endereço IP. Quem faz essa tarefa é um protocolo conhecido como ARP (*Address resolution Protocol*), protocolo que estudamos em aulas anteriores.

Leitura Complementar

Saiba mais sobre IPv6 em <http://ipv6.br/post/introducao/>.

Nesse site, você encontrará maiores informações sobre a motivação da criação do IPv6, bem como detalhes sobre essa nova versão do protocolo IP.

Aproveite e visite também a página Questões Frequentes (FAQ) desse site, em que várias dúvidas são esclarecidas.

Resumo

Estudamos nesta aula que o protocolo de controle utilizado na camada de redes, e alguns comandos que são usados para testar as funcionalidades da rede, assim como as da própria máquina. Você aprendeu ainda as diferenças entre o IPv4 e o IPv6 e conheceu mais detalhes do datagrama IPv6. Você viu ainda que os roteadores possuem tabelas que contêm informações a respeito das redes existentes e qual o próximo roteador no caminho para cada uma delas.

Autoavaliação

1. Pesquise como anda a adoção do IPv6 na internet.
2. Destaque a importância de protocolos de controle como o ICMP.

[Respostas](#)

Respostas

1. A adoção do protocolo IP na sua versão 6 (IPv6) está atualmente em gradativa implantação. No momento (2016), o Google calcula que 13% do tráfego total na Internet utiliza o IPv6. No link abaixo é possível monitorar o grafico de adoção deste protocolo:
<https://www.google.com/intl/pt-BR/ipv6/statistics.html>
2. Protocolos de controle como o ICMP permitem a troca de mensagens de controle, configuração e relatórios de erros entre *hosts* e também entre dispositivos de rede que operam na camada de rede, tais como roteadores e *switches* nível 3.

Referências

KUROSE, J.; ROSS, K. **Redes de computadores e a internet**. 5. ed. São Paulo: Addison Wesley, 2010.

TANENBAUM, Andrew S. **Redes de computadores e a internet**. 4 ed. Rio de Janeiro: Editora Elsevier, 2003.

SOARES, I. F. G. **Redes de computadores das LANs, MANs e WANs às redes ATM**. 2. ed. São Paulo: Editora Campus, 1995.

FOROUZAN, B. **Comunicação de Dados e Redes de Computadores**. 3. ed. Porto Alegre: Bookman, 2006.