

Parte 1

Introdução

O conteúdo desta aula versa sobre a camada 4 – aplicação do modelo TCP/IP e o endereçamento por meio de nomes, bem como sua resolução. São tratadas também a estruturação dos nomes, os domínios e o registro de domínios na internet.

Leitura recomendada:

- Tanenbaum, 2011 – Seções 1.6 e 7.1.
- Kurose, 2003 – Seção 2.5.

Contextualizando:

O que é o DNS?

O DNS – *Domain Name System* ou sistema de nomes de domínio é uma aplicação que realiza o serviço de identificação de computadores na rede por meio de um nome. O DNS atende as outras aplicações, permitindo o uso de endereços da camada de aplicação – URLs ou um endereço de e-mail – ao invés de endereços lógicos da camada de rede (endereço IP). Diferentemente das pessoas, a rede identifica os computadores por seu endereço IP, totalmente numérico e de difícil memorização. Por causa disto é necessário um serviço que possa relacionar um nome de domínio ou de um host à um endereço IP: este serviço é o DNS.

As pessoas preferem guardar nomes ao invés de números. O que é mais fácil de memorizar: **ava.uninter.com** ou **200.150.68.244**?

Para as redes pequenas uma simples tabela contendo os nomes e os respectivos endereços IP dos hosts é suficiente, como era no início da Internet. Assim cada host mantém sua própria tabela local e consegue endereçar toda a rede. Porém com um número imenso de hosts, como é atualmente, é impraticável esta solução, pois haveria necessidade de uma enorme tabela. Além disso seria inviável atualizar as tabelas *hosts* de todos os hosts ao mesmo tempo, cada vez que uma mudança ocorresse. Uma solução seria armazenar uma única tabela em um host específico: isto, porém, geraria um tráfego enorme na rede, além de sobrecarregar este computador. Outra solução seria dividir o grande volume de informações para diversos hosts, que passam a atender a consulta daqueles que necessitam converter nomes em endereços. Estes hosts passam a atuar como **servidores DNS** e estão organizados em uma hierarquia dentro do *name space* ou espaço de nomes. Um espaço de nomes é uma relação única, em toda a rede, entre um nome e um endereço IP. Um espaço de nome pode ser **PLANO** ou **HIERÁRQUICO**. Um espaço de nomes plano contém um nome qualquer – uma sequência de caracteres,

como **servidor_da_rede**, por exemplo – associado a um endereço IP. Isto inviabiliza o seu uso em redes grandes e complexas, pois pode gerar ambiguidades ou nomes duplicados. Um espaço de nomes hierárquico contém nomes compostos de várias partes, cada qual fazendo referência à uma característica ou localização do host. Esta é a forma utilizada na internet, na qual as partes dos nomes são organizadas no formato de uma árvore invertida, formando assim os espaços de nomes de domínio.

Esta “árvore” de domínios comporta até 128 níveis, partindo da raiz – nível 0 –até o nível mais baixo – nível 127. Cada nó ou subdivisão da árvore é identificado por um rótulo (*label*) exclusivo que não se repetirá naquele nível. Uma sequência de rótulos separadas por pontos “.” forma um nome de domínio, como no exemplo dado: **ava.uninter.com**. A leitura e a formação do nome de domínio são sempre feitas de baixo para cima na árvore.

Os domínios podem ser genéricos – por especialidade – como “.edu”, “.com”, “.net”, por área geográfica ou país, como “.br”, “.ch”, “.ar” para Brasil, China e Argentina, por exemplo, sempre utilizando duas letras. Há também os domínios reversos, cuja finalidade é associar um IP a um nome. Neste caso o endereço IP faz parte do nome, porém é escrito ao contrário, e associado aos nomes “arpa” e “in-addr”, como por exemplo em **10.20.30.130.arpa.in-addr**, que se refere ao endereço 130.30.20.10.

Os domínios contêm diversos servidores de DNS, sendo o principal chamado de servidor DNS RAIZ. Este servidor define uma ZONA, à qual estão vinculados todos os demais servidores DNS primários e secundários. O servidor primário armazena e mantém atualizada a tabela de nomes do domínio, enquanto o servidor secundário mantém uma cópia desta tabela para atuar em caso de falha do servidor primário.

Para que um nome possa figurar em um servidor de domínio é necessário que seja cadastrado em uma entidade registradora homologada pela ICANN - *Internet Corporation for Assigned Names and Numbers* – Corporação da Internet para Designação de Nomes e Números. No Brasil o cadastro é mantido pelo **registro.br** aos cuidados da FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo. Juntamente com o **nic.br** – Núcleo de Informações e Coordenação do Ponto BR este cadastro define os nomes de domínio para o território brasileiro.

Como funciona o DNS

O DNS consiste em uma aplicação cliente/servidor. Um host executando o módulo cliente encaminha uma **mensagem de consulta** à um host executando o servidor – ou um servidor DNS. A mensagem compõe-se de um cabeçalho com as informações do cliente e uma seção de perguntas, que contém os nomes de domínios a serem traduzidos para endereços IP. O servidor DNS devolve uma **mensagem de resposta** formada pelo cabeçalho, com as informações do cliente e do servidor, a seção

de perguntas, uma seção de respostas, uma seção de autoridades e uma seção de informações adicionais.

O que acontece se um servidor primário não conseguir resolver um determinado nome? Ele repassará aos nós superiores da hierarquia do domínio para que estes resolvam o nome. Caso a solicitação chegue até o servidor raiz sem a descoberta do IP, um erro será devolvido na mensagem de resposta.

Pesquisa

Existem vários servidores de DNS públicos, como o do Google, cujo IP é 8.8.8.8. Descubra outros e informe os seus nomes e os IPs a seus colegas de curso através do fórum ENDEREÇAMENTO.

DDNS – *Dynamic Domain Name System*

O sistema de nomes de domínio dinâmico – DDNS é uma evolução do DNS devido às constantes mudanças nas redes, com a inclusão de novos hosts e domínios ou eliminação de hosts ou domínios. Promover uma atualização de grande escala é inviável de forma manual. No DDNS, quando um nome é resolvido as informações são enviadas por meio de DHCP para o servidor primário do domínio, que cuida da replicação deste novo conjunto para os demais servidores, incluindo os servidores de DNS secundários. Para evitar o uso inadequado o DDNS pode usar mecanismos de autenticação, garantindo que somente servidores autorizados possam publicar as mudanças.

DNSSEC – *Domain Name System Secure*

O sistema de nomes de domínio seguro é uma versão de DNS que utiliza a criptografia e a assinatura digital para a manutenção e o acesso à base de dados do sistema. O uso deste tipo específico de serviço tem por objetivo evitar ataques de DNS forjado.

Pesquisa

Onde é usado o DNSSEC e com que finalidade? O que é um ataque de DNS forjado? Pesquise e discuta com os colegas no fórum ENDEREÇAMENTO.

DNS – Características

O DNS pode usar tanto o TCP quanto o UDP, e faz as conexões através da porta 53. Para pacotes de mensagem de resposta cujo tamanho não exceda os 512 bytes – tamanho típico de um pacote UDP – este protocolo, o UDP, será usado. Caso o tamanho da mensagem de resposta ultrapasse os 512 bytes ou não seja conhecido o tamanho, então será usada uma conexão TCP.

Parte 2

Introdução

O conteúdo desta aula versa sobre a camada 4 – aplicação do modelo TCP/IP e a utilização de aplicações para *login* em outro host, transferência de mensagens entre host – o correio eletrônico ou e-mail e a transferência de arquivos entre hosts.

Leitura recomendada:

- Tanenbaum, 2011 – Seção 7.2
- Kurose, 2003 – Seção 2.3 e 2.4

TELNET

O programa aplicativo cliente/servidor TELNET – de **TERminal NETwork** é uma aplicação para serviços de terminal virtual que provê uma conexão a um sistema remoto por meio da rede. É a aplicação padrão do TCP/IP para os serviços de terminal virtual de acordo com a ISO – *International Standard Organization*. O TELNET permite que um host crie, por meio de terminal local, uma conexão a um host remoto, fazendo com que este terminal se comporte como se fosse um terminal do sistema remoto. Um terminal, neste cenário, é um dispositivo composto de Teclado, Monitor e Mouse – ou um computador emulando terminal – que possibilita a interação do usuário com os sistemas do computador remoto. O uso de terminal é típico de sistemas operacionais de tempo compartilhado - Time sharing – como o UNIX e o LINUX. O TELNET provê uma interface universal chamada NVT – Network Virtual Terminal – que utiliza um conjunto de caracteres padrão, pois hosts diferentes podem usar diferentes conjuntos de caracteres, em função do idioma ou do sistema operacional utilizado por cada um.

Para tratar os diferentes recursos existentes em cada host o TELNET permite ao cliente e o servidor negociarem as opções de configuração antes do uso do serviço. Estas opções são recursos extras disponíveis para terminais mais sofisticados, como cores, gráficos e teclas de função ou aceleradoras. O TELNET faz a conversão de caracteres de acordo com o tipo de computador acessado, por meio de um driver específico. Para estabelecer a comunicação com o host remoto o TELNET usa uma conexão TCP e a porta 23 do servidor. O funcionamento do TELNET ocorre de três modos de operação:

- O modo **Padrão**, utilizado quando nenhum outro modo for negociado, e aquele no qual o eco é local, isto é, uma vez digitado um caractere, o próprio cliente (terminal local) faz a

apresentação do mesmo na tela, porém só transmite para o servidor (host remoto) a linha inteira (ou até que pressionada a tecla <ENTER>).

- No modo **Caractere** cada vez que um caractere é digitado o mesmo é enviado ao servidor, que o retransmite de volta para que o cliente faça a apresentação na tela. Isto gera dois efeitos: em conexões mais lentas ou congestionadas, pode haver um retardo entre a digitação e a apresentação do caractere; além disso cada caractere digitado vai gerar três segmentos de TCP na rede.
- No modo **Linha** a edição de linhas (eco, correção, etc.) é realizada pelo cliente. Quando finalizada a edição pela tecla <ENTER> então toda a linha é enviada para o servidor.

CORREIO ELETRÔNICO

Uma das aplicações mais conhecidas da internet é o correio eletrônico, ou o E-mail (do Inglês *Electronic Mail*). No início da era da internet era possível trocar mensagens curtas e somente de texto entre dois hosts distantes. Atualmente as mensagens de e-mail são compostas de texto, áudio, imagem e vídeo, e podem ser encaminhadas a vários destinos simultaneamente. O serviço de correio eletrônico usa uma arquitetura com três componentes principais, a saber:

- O *User Agente* (UA), agente de usuário, é o serviço ou aplicação responsável pelas operações do e-mail no cliente, seja o remetente ou o destinatário;
- O *Message Transfer Agent* (MTA), agente de transferência de mensagens, é a aplicação cliente/servidor que responde pelo envio de mensagens à um servidor de correio eletrônico;
- *Message Access Agent* (MAA), agente de acesso às mensagens, é a aplicação cliente/servidor responsável por buscar as mensagens em um servidor de e-mail.

Um serviço de Correio Eletrônico pode operar de quatro modos distintos. No primeiro modo, o remetente e destinatário estão conectados no mesmo sistema. Neste caso é necessário apenas o uso dos programas User Agent (UA). O remetente faz uso do UA para preparar e encaminhar seu e-mail para o destinatário, e quando usar seu UA, receberá a mensagem. É o caso típico do serviço “mail” do UNIX / LINUX.

Em um segundo modo, o remetente e destinatário estão conectados a sistemas distintos. Então é necessário o uso de dois programas User Agent (UA) e um par de programas Message Transfer Agent (MTA), que funcionam em um modelo cliente/servidor para encaminhar a mensagem de um sistema ao outro. Este é o caso de uma mensagem de e-mail trocada entre dois sistemas UNIX / LINUX conectados à rede.

Em um terceiro modo o Remetente faz parte de uma LAN / WAN e o destinatário está conectado diretamente ao serviço de correio eletrônico. Neste modo é necessário o uso de dois programas User Agent (UA) e dois pares de servidores *Message Transfer Agent*, cada par funcionando em modelo cliente / servidor para o encaminhamento da mensagem de um sistema até o outro.

Finalmente, no quarto modo, o remetente e destinatário estão conectados ao serviço de correio eletrônico por meio de uma LAN / WAN. É necessário o uso de dois programas User Agent (UA), dois pares de servidores Message Transfer Agent (MTA) e um par de servidores Message Access Agent (MAA). Este é o cenário típico atualmente na internet

SMTP – Simple Mail Transfer Protocol

O SMTP - *Simple Mail Transfer Protocol* ou Protocolo Simples de Transferência de Mensagem é o protocolo que define a comunicação entre cliente e servidor do *Message Transfer Agent* (MTA). O SMTP utiliza a porta 25 (conexão em texto plano)¹ ou a porta 465 (conexão criptografada via SSL). Em um processo típico de envio de e-mail o SMTP é utilizado tanto entre o cliente (UA) e o servidor de correio quanto entre os servidores de correio MTA).

POP3 – Post Office Protocol versão 3

O POP3 – *Post Office Protocol* versão 3 ou Protocolo de Posto de Correio é o protocolo que define a comunicação entre cliente e servidor *Message Access Agent* (MAA) para acessar as mensagens deixadas em um servidor de e-mail. O POP3 acessa as mensagens no servidor de e-mail e as disponibiliza para o UA apresentá-las ao seu destinatário. O POP3 permite o acesso em dois modos, o modo *keep* e o módulo *delete*. No modo *keep* as mensagens são acessadas, porém mantidas no servidor de e-mail, e, portanto, podem ser acessadas novamente a partir de outro cliente MAA. No modo *delete* as mensagens são acessadas e excluídas do servidor de e-mail, sendo mantidas no UA a partir deste ponto. O POP3 utiliza a porta 110 do TCP para acessar as mensagens de correio eletrônico em um servidor.

¹ No Brasil o CGI.BR orientou, em 2012, usuários, provedores e operadoras de internet a utilizar a porta 587. O intuito é uma medida de segurança para diminuir o número de spams: <http://www.cgi.br/noticia/cgi-br-anuncia-ultima-etapa-da-campanha-para-diminuir-numero-de-spams-enviados-por-redes-brasileiras/309>.

IMAP4 – Internet Mail Access Protocol versão 4

O IMAP – *Internet Mail Access Protocol* ou Protocolo de Acesso a Correio pela Internet é o protocolo que define a comunicação entre cliente e servidor *Message Access Agent* (MAA) de forma similar ao POP3, porém com muitos recursos adicionais, como por exemplo:

- É possível acessar o assunto de um e-mail antes de transferi-lo para o UA;
- É possível pesquisar um conteúdo específico nos e-mails do servidor;
- É possível baixar parcialmente um e-mail (sem as imagens, vídeos ou anexos, por exemplo);
- Também é possível que o usuário gerencie pastas e defina o armazenamento de suas mensagens nestas pastas no servidor de e-mail.

O IMAP4 utiliza a porta 143 do TCP para as conexões cliente / servidor com o servidor de e-mail.

TRANSFERÊNCIA DE ARQUIVOS - FTP – *File Transfer Protocol*

O FTP – *File Transfer Protocol* ou Protocolo de Transferência de Arquivos é o protocolo padrão do TCP/IP para transferência de arquivos entre hosts. É uma aplicação cliente / servidor que estabelece duas conexões entre os hosts: uma para os dados e outra para o controle da transferência, e utiliza as portas 20 e 21 para estas duas conexões. Para acessar o servidor e fazer uma transferência é necessário ter uma conta com um nome de usuário (login) e uma senha. A transmissão dos dados do FTP é feita por uma conexão TCP. É possível utilizar também o FTP Anônimo para arquivos de acesso público. Neste caso, geralmente não é necessário login e senha, porém o padrão é que sejam:

Login: **anonymous**

Senha: **guest**

Nestes casos o acesso ao sistema é restrito e poucas operações são permitidas.

Outra alternativa para o FTP é o TFPT - *Trivial File Transfer Protocol*, um protocolo de transferência de arquivos muito simples e muito semelhante ao FTP. É muito utilizado para transferir pequenos arquivos entre hosts de uma rede, como, por exemplo, quando um terminal remoto ou um cliente inicia o seu funcionamento, a partir do servidor.

Pesquisa

O FTP é utilizado por diversos serviços para a transferência de arquivos. Você consegue identificar quais são estes outros?

Trocando Ideias

Acesse o fórum sobre APLICAÇÕES e compartilhe suas descobertas, suas experiências, exponha suas dúvidas.... Faça contato com seus colegas de curso e de turma por meio do fórum e discuta o que aprendeu. Esclareça suas dúvidas.

Síntese

Nessa aula foram apresentados os protocolos e serviços da camada de aplicação voltados para o acesso remoto via terminal, o correio eletrônico e a transferência de arquivos entre hosts.

Compartilhando

Que tal compartilhar o que você aprendeu? Acesso o fórum sobre as aplicações e discuta com seus colegas de curso e de trabalho. Procure reforçar o entendimento sobre o conteúdo apresentado.

Autoavaliação

- Para que poderia ser usado o TELNET?
- O que é possível “negociar” em uma conexão TELNET?
- Qual é a função de um UA – *User Agent* no correio eletrônico?
- Porque necessita-se de POP3 e IMAP4 nos serviços de correio eletrônico?
- Quantas conexões o FTP utiliza para a transferência de arquivos? Qual a finalidade destas conexões?

Referências

Tanenbaum, Andrew S.; Wetheral, David. **Redes de Computadores - 5ª edição**. São Paulo. Pearson, 2011.

Kurose, James F.; Ross, Keith W. **Redes de Computadores e a Internet: uma nova abordagem**. São Paulo. Pearson, 2003.