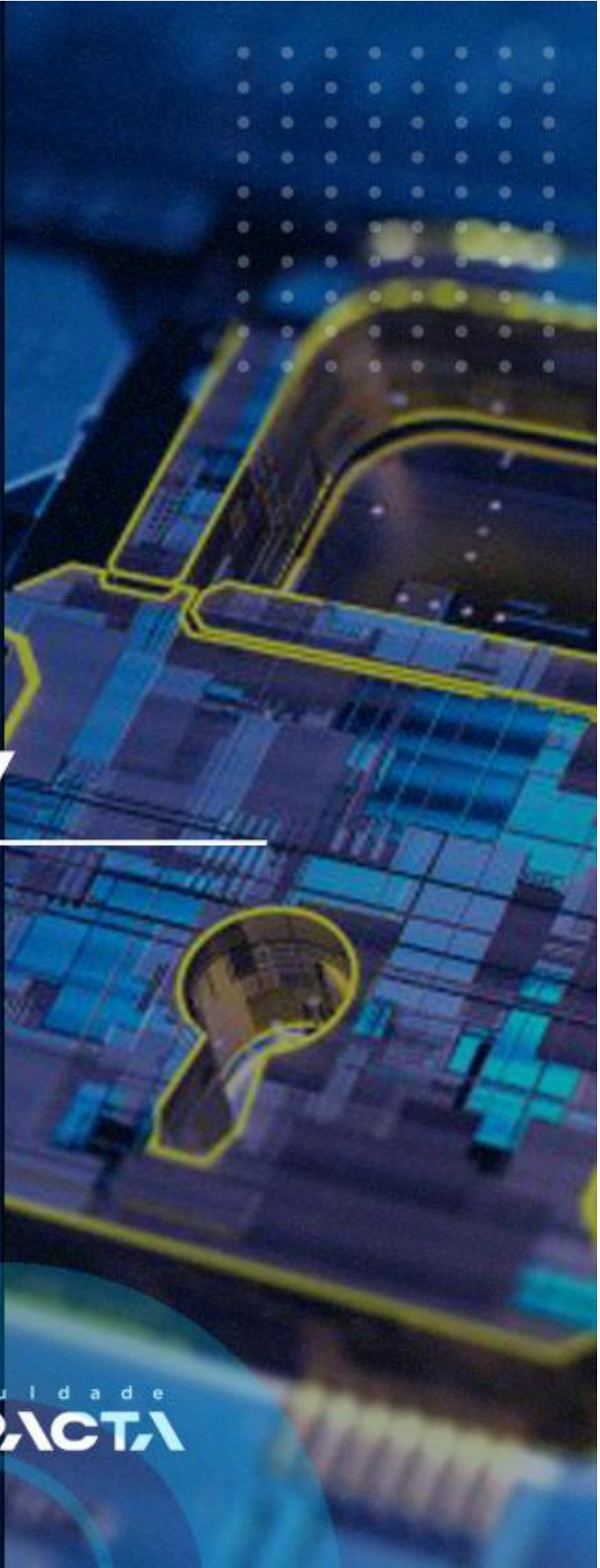
NEaD
Núcleo de Educação a Distância

CYBER SECURITY



Faculdade IMPACTA

4

Entendendo a PDU do protocolo ARP e a camada de transporte

Alex Sandro da Silva Feitosa

Resumo

Nessa aula, abordaremos conceitos relacionados à camada de transporte, explicando de forma geral como ela gerencia a entrega de dados entre dispositivos na rede. Também falaremos sobre a comunicação sem fio, destacando sua importância e aplicação no dia a dia. Por fim, trataremos brevemente da segurança da infraestrutura de rede, reforçando a necessidade de proteger as informações que trafegam pelos sistemas de comunicação.

Introdução

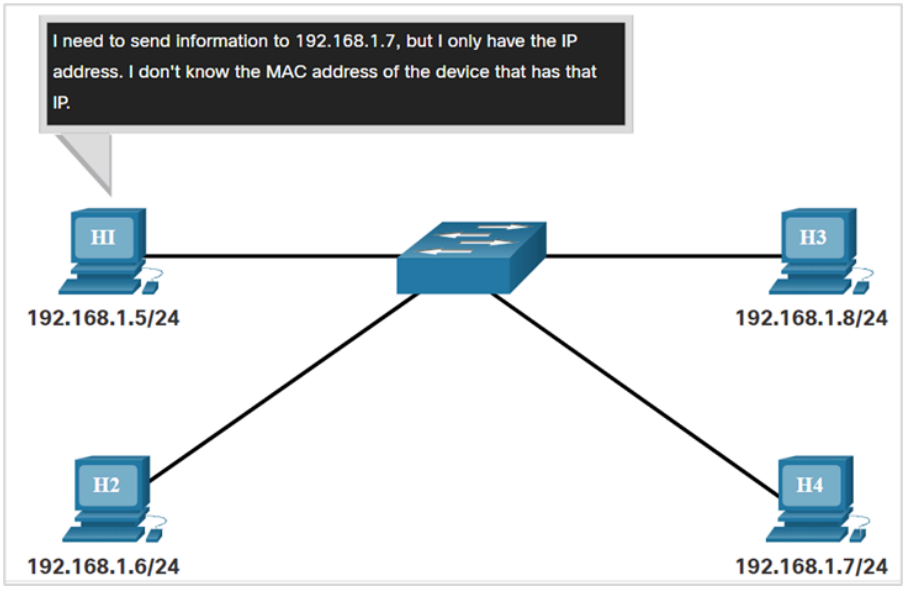
Vamos abordar de forma geral a camada de transporte, entendendo como ela gerencia a entrega de dados entre dispositivos. Também falaremos sobre a comunicação sem fio, destacando sua presença no dia a dia. Por fim, será tratada brevemente a importância da segurança nas redes.

1.1. Analisar a PDU do protocolo ARP

1.1.1 ARP - Visão geral

A figura ilustra um problema ao enviar um pacote para outro host na mesma rede IPv4 local porque o endereço IP é conhecido, mas o endereço MAC do dispositivo é desconhecido.

Figura 1.1 MAC



Fonte: CCNA Cyber OPS Associate v1, 2020.

Um dispositivo utiliza o protocolo ARP (Address Resolution Protocol) para determinar o endereço MAC de destino de um dispositivo local quando conhece o endereço IPv4.

O ARP fornece duas funções básicas:

Resolução de endereços IPv4 em endereços MAC

Mantendo uma tabela de mapeamentos de endereços IPv4 para MAC

Quando um pacote é enviado para a camada de enlace de dados para ser encapsulado em um quadro Ethernet, o dispositivo consulta uma tabela chamada tabela ARP ou cache ARP em sua memória RAM para encontrar o endereço MAC mapeado para o endereço IPv4.

O dispositivo de envio pesquisará em sua tabela ARP um endereço IPv4 de destino e um endereço MAC correspondente, se o endereço IPv4 de destino do pacote estiver na mesma rede que o endereço IPv4 de origem.

Se o dispositivo localizar o endereço IPv4, o endereço MAC correspondente será usado como o endereço MAC destino no quadro.

Quando um dispositivo precisa determinar o endereço MAC mapeado para o endereço IPv4 e nenhuma entrada é encontrada para o endereço IPv4 em sua tabela ARP, uma solicitação ARP é enviada.

Somente o dispositivo com o endereço IPv4 de destino associado à solicitação ARP responderá com uma resposta ARP.

Para cada dispositivo, um temporizador de cache ARP remove as entradas ARP que não foram usadas por um período de tempo especificado.

Os horários diferem dependendo do sistema operacional do dispositivo.

Os comandos também podem ser usados para remover manualmente algumas ou todas as entradas na tabela ARP.

Após a remoção de uma entrada, o processo de envio de uma requisição ARP e de recebimento de uma resposta ARP deve ocorrer novamente para inserir o mapa na tabela ARP.

Em um roteador Cisco, o comando show ip arp é usado para exibir a tabela ARP.

Figura 1.2 MAC

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1            -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225          -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226          1   a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

Fonte: CCNA Cyber OPS Associate v1, 2020.

Em um PC Windows 10, o comando arp –a é usado para exibir a tabela ARP.

Figura 1.3 MAC

```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
  192.168.1.110         08-3e-0c-f5-f7-56     dynamic
  192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
  192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
  192.168.1.126         24-77-03-45-5d-c4     dynamic
  192.168.1.146         94-57-a5-0c-5b-02     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

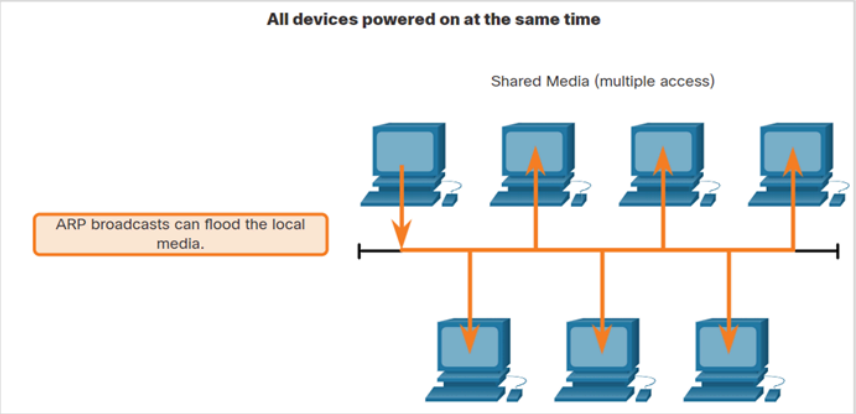
Fonte: CCNA Cyber OPS Associate v1, 2020.

1.1.2 Problemas de ARP

A figura ilustra um problema ao enviar um pacote para outro host na mesma rede IPv4 local porque o endereço IP é conhecido, mas o endereço MAC do dispositivo é desconhecido.

Broadcasts ARP

Figura 1.4 MAC



Fonte: CCNA Cyber OPS Associate v1, 2020.

Como um quadro broadcast, uma requisição ARP é recebida e processada por todos os dispositivos na rede local.

Em uma rede comercial típica, essas transmissões teriam um impacto mínimo no desempenho da rede.

Se muitos dispositivos começarem a acessar serviços de rede ao mesmo tempo, pode haver redução no desempenho por um curto período de tempo.

Depois que os dispositivos enviarem os broadcasts ARP iniciais e tiverem reconhecido os endereços MAC necessários, qualquer impacto na rede será minimizado.

1.1.3 Falsificação ARP (ARP Spoofing)

O uso de ARP pode levar a um risco potencial de segurança em alguns casos.

Um agente de ameaça usa ARP spoofing para realizar um ataque de envenenamento ARP.

É uma técnica usada por um agente de ameaça para responder a uma solicitação ARP de um endereço IPv4 pertencente a outro dispositivo, como o gateway padrão.

O agente da ameaça envia uma resposta ARP com seu próprio endereço MAC. O receptor da resposta do ARP adicionará o endereço MAC errado à sua tabela ARP e enviará esses pacotes ao agente da ameaça.

1.2. Camada de transporte

1.2.1 Papel da camada de transporte

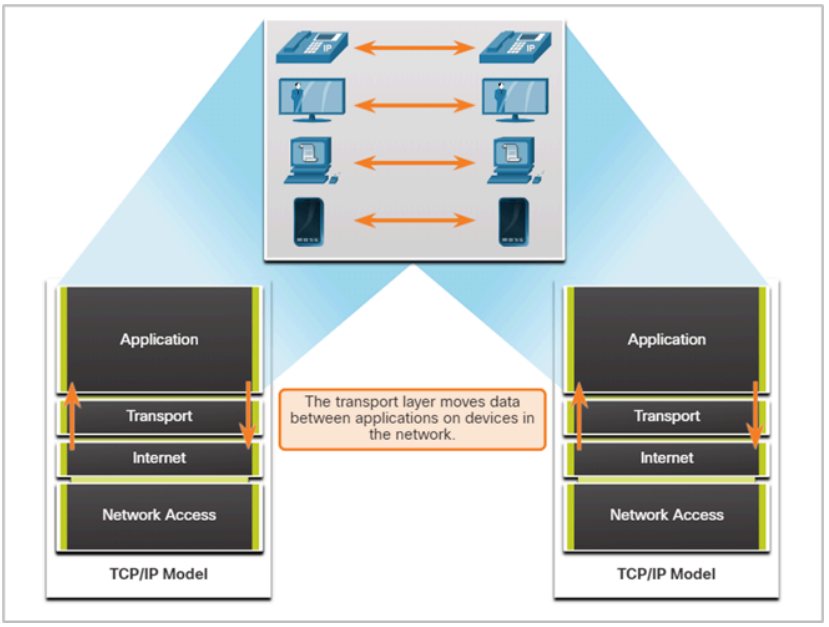
A figura ilustra um problema ao enviar um pacote para outro host na mesma rede IPv4 local porque o endereço IP é conhecido, mas o endereço MAC do dispositivo é desconhecido.

Na camada 4 do modelo OSI Transporte, tratamos da comunicação lógica entre sistemas executados entre hosts.

Como mostra a figura 1.5, a camada de transporte é o link(enlace de comunicação) entre a camada de 7 e as camadas inferiores que são responsáveis pela transmissão na rede.

A camada 4 do modelo OSI Transporte inclui dois protocolos, Transmission Control Protocol (TCP) e User Datagram Protocol (UDP).

Figura 1.5 MAC



Fonte: CCNA Cyber OPS Associate v1, 2020.

A camada 4 do modelo OSI Transporte tem algumas responsabilidades.

Rastreamento de Conversações Individuais

Cada conjunto de dados fluindo entre um aplicativo de origem e um aplicativo de destino é conhecido como uma conversa e é rastreado separadamente.
É responsabilidade da camada de transporte manter e monitorar essas várias conversações.
Conforme mostrado na figura, um host pode ter vários aplicativos que se comunicam pela rede simultaneamente.
A maioria das redes tem uma limitação da quantidade de dados que pode ser incluída em um único pacote. Os dados devem ser divididos em partes gerenciáveis (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

Segmentação de Dados e Remontagem de Segmentos

É responsabilidade da camada de transporte dividir os dados do aplicativo em blocos de tamanho adequado.
Dependendo do protocolo de camada de transporte usado, os blocos de camada de transporte são chamados de segmentos ou datagramas.
A figura mostra a camada de transporte usando blocos diferentes para cada conversa.
A camada de transporte divide os dados em blocos menores (segmentos ou datagramas) que são mais fáceis de gerenciar e transportar.
Adicionar Informações de Cabeçalho
O protocolo da camada de transporte também adiciona informações de cabeçalho contendo dados binários organizados em vários campos a cada bloco de dados.

Os valores nesses campos permitem que vários protocolos da camada de transporte executem funções diferentes no gerenciamento da comunicação de dados.
As informações do cabeçalho são usadas pelo host receptor para remontar os blocos de dados em um fluxo de dados completo para o programa da camada de aplicativo receptor.
A camada de transporte garante que, mesmo com vários aplicativos em execução em um dispositivo, todos os aplicativos recebam os dados corretos (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

1.2.2 Identificação das Aplicações

A camada de transporte deve separar e gerenciar várias comunicações com as diferentes necessidades de requisitos de transporte.
Para passar fluxos de dados para os aplicativos adequados, a camada de transporte identifica o aplicativo de destino usando um identificador chamado número da porta.
Conforme mostrado na figura, cada processo de software que precisa acessar a rede é atribuído a um número de porta exclusivo para aquele host (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

Multiplexação das Conversas

O envio de alguns tipos de dados por uma rede, como um fluxo de comunicação completo, pode consumir toda a largura de banda disponível.
Isso evita que outras conversas de comunicação ocorram ao mesmo tempo e também dificultam a recuperação de erros e a retransmissão de dados danificados.
Como mostrado na figura, a camada de transporte usa segmentação e multiplexação para permitir que diferentes conversas de comunicação sejam intercaladas na mesma rede.
A verificação de erros pode ser realizada nos dados do segmento, para determinar se o segmento foi alterado durante a transmissão (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

A camada do modelo OSI Transporte inclui os protocolos TCP e UDP.

O TCP fornece confiabilidade e controle de fluxo. Operações básicas de TCP:

Número e rastreamento dos segmentos transmitidos entre hosts específico

Confirmação das informações recebidos

Retransmitir quaisquer informações não identificadas após um período de tempo

Informações de sequência que possivelmente podem chegar em ordem errada

Enviar informações a uma taxa aceitável pelo receptor

O UDP fornece as funções básicas para fornecer datagramas entre os aplicativos apropriados, com muito pouca sobrecarga e verificação de dados.
UDP é um protocolo sem conexão.
O UDP é conhecido como um protocolo de entrega de melhor esforço porque não há confirmação de que os dados são recebidos no destino.
O UDP também é usado por aplicativos de solicitação e resposta onde os dados são mínimos, e a retransmissão pode ser feita rapidamente.

> Se for importante que todos os dados cheguem e que possam ser processados em sua sequência adequada, TCP é usado como protocolo de transporte (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

Portas de Comunicação: As portas de comunicação definidas para o destino informam o aplicativo que está usando a transmissão. Já as portas de origem só definem em que porta o destino deve responder as confirmações de recebimento dos datagramas. Essas portas são divididas em categorias, conforme descritas abaixo:

Conhecidas - 0 a 1023

Aplicativos públicos = 0 a 255

Aplicativos comerciais = 256 a 1023

Registradas - 1024 a 49151

Dinâmicas/Privadas - 49152 a 65535

As portas conhecidas foram estabelecidas e documentadas pelo IANA, portanto não podem ser usadas sem prévia autorização do mesmo. As portas registradas e dinâmicas são reconhecidas pelo IANA, mas são de uso livre, não requerendo autorização prévia, essas portas costumam ser chamadas de portas não regulamentadas.

Porta da Origem: Atribuída dinamicamente usando os números de portas não regulamentadas.

Porta de Destino: Atribuídas de acordo com o protocolo de camada superior em uso, portanto usando as portas conhecidas.

OBS: Com o uso do comando "netstat -n" no prompt de comando do DOS é possível verificar as comunicações em andamento do Micro e as portas em uso.

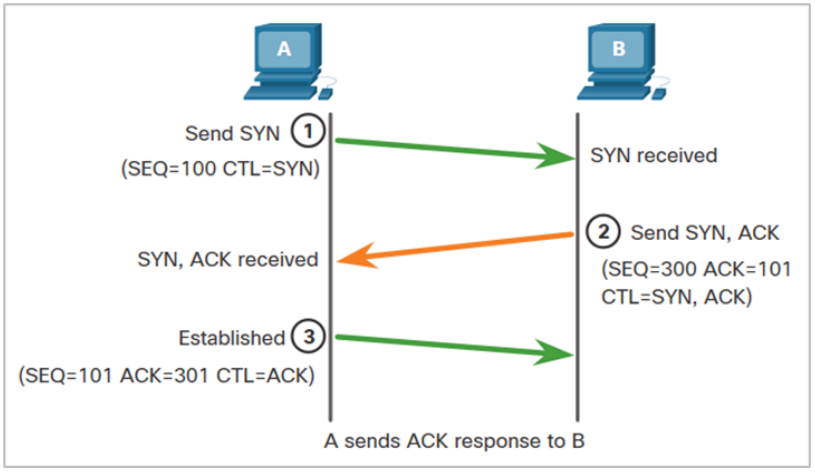
1.2.3 Estabelecimento de conexão TCP

Em uma conexão TCP, o cliente estabelece a conexão com o servidor usando o processo handshake de três vias.

O handshake de três vias válidas se o host de destino está disponível para comunicação.

> **As etapas de estabelecimento da conexão TCP são:**
> **Etapa 1.** SYN: O cliente inicial solicita uma sessão de comunicação cliente-servidor com o servidor.
> **Etapa 2.** ACK e SYN: O servidor reconhece a sessão de comunicação cliente-servidor e solicita uma sessão de comunicação servidor-cliente.
> **Etapa 3.** ACK: O cliente inicial reconhece a sessão de comunicação entre o servidor e o cliente (Cisco NetAcademy CCNA Cyber OPS Associate v1 2021).

Figura 1.6 MAC



Fonte: CCNA Cyber OPS Associate v1, 2020.

Término da Sessão:

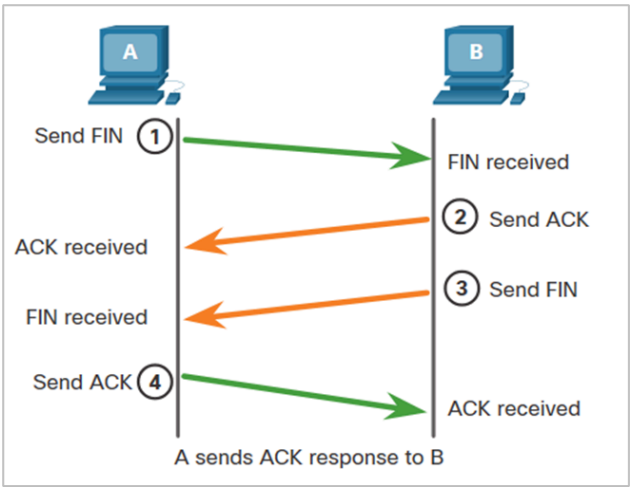
Para fechar uma conexão, o flag de controle Finish (FIN) deve ser ligado no cabeçalho do segmento.

Para terminar cada sessão TCP de uma via, um handshake duplo, consistindo de um segmento FIN e um segmento ACK (Acknowledgment) é usado.

Portanto, para terminar uma conversação única permitida pelo TCP, quatro trocas são necessárias para finalizar ambas as sessões. O cliente ou o servidor podem iniciar o encerramento.

As etapas de encerramento da sessão são:
Etapa 1. FIN: Quando o cliente não tem mais dados para enviar no fluxo, ele envia um segmento com o sinalizador FIN definido.
Etapa 2. ACK: O servidor envia um ACK para confirmar o recebimento do FIN para encerrar a sessão do cliente para o servidor.
Etapa 3. FIN: O servidor envia um FIN ao cliente para encerrar a sessão servidor para cliente.
Etapa 4. ACK: O cliente responde com um ACK para reconhecer o FIN do servidor(Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

Figura 1.7 MAC

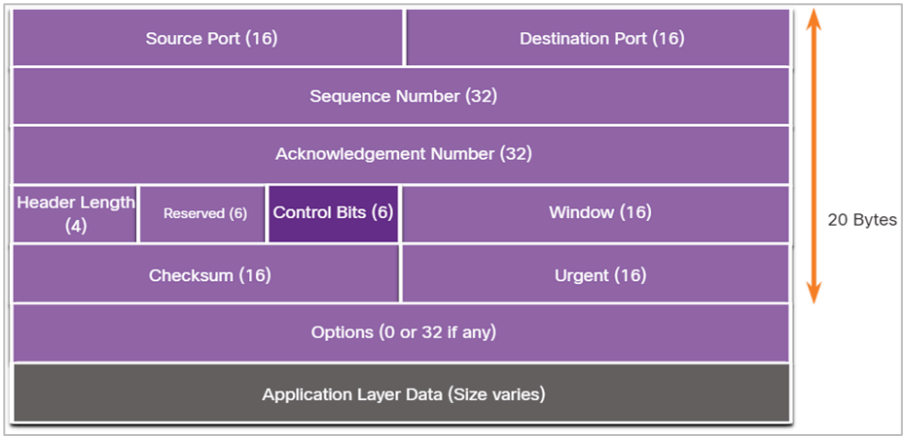


Fonte: CCNA Cyber OPS Associate v1, 2020.

1.2.4 Análise de handshake TCP de três vias

Os hosts mantêm o estado, rastreiam cada segmento de dados em uma sessão e trocam informações sobre os dados recebidos usando as informações no cabeçalho TCP.
O TCP é um protocolo full-duplex, em que cada conexão representa duas sessões de comunicação unidirecional. Para estabelecer uma conexão, os hosts realizam um handshake triplo (three-way handshake). Conforme mostrado na figura, os bits de controle no cabeçalho TCP indicam o progresso e o status da conexão.
As funções do handshake de três vias são:
Estabelece que o dispositivo de destino está presente na rede.
Ele verifica se o dispositivo de destino possui um serviço ativo e está aceitando solicitações no número da porta de destino que o cliente inicial pretende usar.
Ele informa ao dispositivo de destino que o cliente de origem pretende estabelecer uma sessão de comunicação nesse número de porta.
Após a conclusão da comunicação, as sessões são fechadas e a conexão é encerrada. Os mecanismos de conexão e sessão ativam a função de confiabilidade do TCP.
Os seis bits no campo Bits de Controle do cabeçalho do segmento TCP são também conhecidos como flags. Um sinalizador é um pouco definido como ativado ou desativado. Os seis bits de controle sinalizadores são os seguintes:
URG - Campo indicador de urgência
ACK - Indicador de confirmação usado no estabelecimento de conexão e encerramento de sessão
PSH - Função Push
RST - Redefina a conexão quando ocorrer um erro ou tempo limite
SYN - Sincronizar números de sequência usados no estabelecimento de conexão
FIN - Não há mais dados do remetente e usados no encerramento da sessão (Cisco NetAcademy CCNA Cyber OPS Associate v1, 2021).

Figura 1.8 MAC



Fonte: CCNA Cyber OPS Associate v1, 2020.

1.3. Serviços de rede

1.3.1 DHCP - Dynamic Host Configuration Protocol

Dois tipos de endereçamento:

- Dinâmico - o protocolo DHCP (Dynamic Host Configuration Protocol) para serviço IPv4 automatiza a atribuição de endereços IPv4, máscaras de sub-rede, gateways e outros parâmetros de rede IPv4.
- Estático - O administrador da rede insere manualmente as informações do endereço IP nos hosts.

Quando um host se conecta à rede, o servidor DHCP escolhe um endereço de um intervalo configurado de endereços denominado pool e o atribui ao host.

O DHCP pode alocar endereços IP por um período de tempo configurável, chamado período de concessão.

Operação do DHCP

A operação DHCP inclui: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK e DHCPNAK.

Quando o dispositivo configurado com DHCP se conecta à rede, o cliente transmite uma mensagem DHCPDISCOVER para identificar quaisquer servidores DHCP disponíveis na rede.

Um servidor DHCP responde com uma mensagem DHCPOFFER, que oferece uma concessão ao cliente.

O cliente envia uma mensagem DHCPREQUEST que identifica o servidor explícito e a oferta de aluguel que o cliente está aceitando.

Se o endereço IPv4 solicitado pelo cliente, ou oferecido pelo servidor, ainda estiver disponível, o servidor retornará a mensagem DHCPACK . Se a oferta não for mais válida, o servidor selecionado responde com uma mensagem DHCPNAK. Se uma mensagem DHCPNAK for retornada, o processo de seleção começará novamente com uma nova mensagem DHCPDISCOVER sendo transmitida.

1.3.2 DNS - Domain Name System

O Sistema de Nomes de Domínio (DNS) fornece nomes de domínio e seus endereços IP associados.

O sistema DNS consiste em uma hierarquia global de servidores distribuídos que contêm bancos de dados de nomes para mapeamentos de endereços IP.

O computador cliente na figura enviará uma solicitação ao servidor DNS para obter o endereço IP de www.cisco.com para que ele possa endereçar pacotes para esse servidor.

O tráfego DNS mal-intencionado pode ser detectado por meio da análise de protocolo e da inspeção de informações de monitoramento de DNS.

A Hierarquia de Domínio DNS

O DNS consiste em uma hierarquia de domínios genéricos de nível superior e vários domínios de nível de país.

Os domínios de segundo nível são representados por um nome de domínio seguido por um domínio de nível superior.

Os subdomínios são encontrados no próximo nível da hierarquia DNS e representam alguma divisão do domínio de segundo nível.

Domínio de quarto nível pode representar um host em um subdomínio.

Os domínios de nível superior representam o tipo de organização ou país de origem. Exemplos: (.org) - uma organização sem fins lucrativos, (.au) - Austrália.

O Processo de Pesquisa de DNS

Para resolver um nome para um endereço IP, o resolvedor, primeiro verificará seu cache DNS local. Se o mapeamento não for encontrado, uma consulta será emitida para o servidor DNS.

Se o mapeamento não for encontrado lá, o servidor DNS consultará outros servidores DNS de nível superior que são autoritativos para o domínio de nível superior para localizar o mapeamento. Estes são conhecidos como consultas recursivas.

Os servidores DNS de cache podem resolver consultas recursivas sem encaminhar as consultas para servidores de nível superior.

Se um servidor exigir dados para uma zona, ele solicitará uma transferência desses dados de um servidor autoritário para essa zona. O processo de transferência de dados DNS entre servidores é conhecido como transferência de zona.

Etapas envolvidas na resolução de DNS:

Etapa 1 - O usuário digita um FQDN no campo Endereço do aplicativo do navegador.

Etapa 2 - Uma consulta DNS é enviada ao servidor DNS designado para o computador cliente.

Etapa 3 - O servidor DNS combina o FQDN com seu endereço IP.

Etapa 4 - A resposta da consulta DNS é enviada de volta ao cliente com o endereço IP do FQDN.

Etapa 5 - O servidor DNS combina o FQDN com seu endereço IP.

Formato de Mensagem DNS

O DNS usa a porta UDP 53 para consultas e respostas DNS.

Se uma resposta DNS exceder 512 bytes, DNS dinâmico (DDNS) é usado.

As comunicações do protocolo DNS usam um único formato denominado mensagem.

O DNS usa o mesmo formato de mensagem para todos os tipos de consultas do cliente e resposta do servidor, mensagens de erro e transferência de informações de registro de recursos.

O Protocolo WHOIS

WHOIS é um protocolo baseado em TCP que é usado para identificar os proprietários de domínios da Internet através do sistema DNS.

O aplicativo WHOIS usa uma consulta, na forma de um FQDN.

O WHOIS é um ponto de partida para identificar locais potencialmente perigosos da Internet que possam ter sido alcançados através da rede.

O ICANN Lookup (https://lookup.icann.org/), uma ferramenta WHOIS baseada na Internet, é usado para obter o registro de um URL.

1.3.3 NAT - Network Address Translation

Para permitir que um dispositivo com endereço IPv4 privado acesse dispositivos e recursos fora da rede local, o endereço privado deve ser traduzido para um endereço público.

O NAT fornece a tradução de endereços privados para endereços públicos.

Um único endereço IPv4 público pode ser compartilhado por milhares de dispositivos, cada um configurado com um endereço IPv4 privado exclusivo.

A solução para a redução do espaço de endereços IPv4 e limitações do NAT é a eventual transição para IPv6.

O NAT é usado para conservar endereços IPv4 públicos.

Os roteadores habilitados para NAT podem ser configurados com um ou mais endereços IPv4 públicos válidos, conhecidos como pool NAT.

Um dispositivo ativado para NAT geralmente opera na fronteira de uma rede stub.

Quando um dispositivo dentro da rede stub deseja se comunicar com um dispositivo fora de sua rede, o pacote é encaminhado para o roteador de fronteira e o roteador executa o processo NAT.

Nota: A conexão com o ISP pode usar um endereço privado ou um endereço público que é compartilhado entre os clientes. Neste módulo, um endereço público é exibido.

Tradução de Endereço de Porta

A conversão do PAT, também conhecida como sobrecarga de NAT, mapeia os endereços IPv4 privados para um único endereço IPv4 público ou para alguns endereços.

Quando um dispositivo inicia uma sessão TCP/IP, ele gera um valor de porta de origem TCP ou UDP ou um ID de consulta especialmente atribuído para ICMP, para identificar, de forma exclusiva, a sessão.

O PAT garante que os dispositivos utilizem um número de porta diferente do TCP para cada sessão com um Servidor na Internet.

O PAT usa números de portas de origem exclusivos no endereço IP global interno para distinguir entre conversões.

1.3.4 E-mail

O e-mail é um método de armazenar, enviar e recuperar mensagens eletrônicas em uma rede.

Os clientes de e-mail se comunicam com os servidores de e-mail para enviar e receber e-mails.

O e-mail suporta três protocolos separados para a operação: SMTP, POP e IMAP.

Um cliente recupera e-mails usando um dos dois protocolos da camada de aplicação: POP ou IMAP.

SMTP

Os formatos de mensagens SMTP exigem um cabeçalho de mensagem e um corpo de mensagem.

Quando um cliente envia um e-mail, o processo SMTP do cliente se conecta a um processo SMTP do servidor em uma porta 25 bem conhecida.

Quando o servidor recebe a mensagem, ele a coloca em uma conta local, se o destinatário for local, ou encaminha a mensagem para outro servidor de correio para entrega.

Periodicamente, o servidor verifica se há mensagens na fila e tenta enviá-las novamente. Se a mensagem ainda não for entregue após um período pré-determinado de expiração, ela é devolvida ao remetente como não entregue.

POP3

POP3 é usado por um aplicativo para recuperar um e-mail de um servidor de e-mail.

Com o POP3, as mensagens de email são baixadas para o cliente e removidas do servidor.

O servidor inicia o serviço POP3 ouvindo passivamente na porta TCP 110 as solicitações de conexão do cliente.

O cliente envia uma solicitação para estabelecer uma conexão TCP com o servidor.

Assim que a conexão for estabelecida, o servidor POP3 enviará uma saudação. O cliente e o servidor POP3 trocam comandos e respostas até que a conexão seja fechada ou abortada.

IMAP

IMAP é o protocolo que descreve um método para recuperar mensagens de e-mail.

Quando o usuário se conecta a um servidor compatível com IMAP, cópias das mensagens são baixadas para o aplicativo cliente. As mensagens originais são mantidas no servidor até serem excluídas manualmente.

Os usuários exibem cópias das mensagens em seu software cliente de e-mail.

Os usuários podem criar uma hierarquia de arquivos no servidor para organizar e armazenar o e-mail.

Quando um usuário decide excluir uma mensagem, o servidor sincroniza essa ação e exclui a mensagem do servidor.

1.3.5 HTTP

Quando um endereço da web ou Uniform Resource Locator (URL) é digitado em um navegador da web, o navegador da web estabelece uma conexão com o serviço da web que está usando o protocolo HTTP.

Vamos dar uma olhada em como uma página da web é aberta em um navegador. Exemplo: http://www.cisco.com/index.html

Etapa 1: o navegador interpreta as três partes do URL:

http (o protocolo ou esquema)

www.cisco.com (o nome do servidor)

index.html (o nome do arquivo específico solicitado)

Etapa 2: O cliente inicia uma solicitação HTTP a um servidor enviando uma solicitação GET ao servidor e solicita o arquivo index.html.

Etapa 3: Em resposta à solicitação, o servidor envia ao navegador o código HTML dessa página da web.

Etapa 4: O navegador decifra o código HTML e formata a página para a janela do navegador.

URLs HTTP podem especificar a porta no servidor que deve manipular os métodos HTTP.

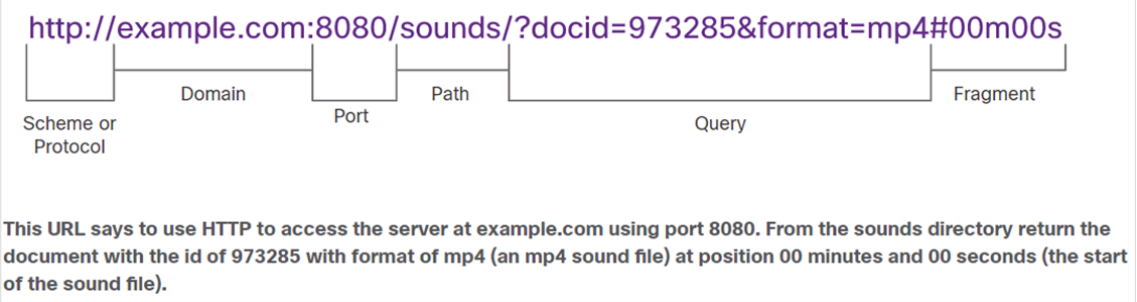
Ele pode especificar uma seqüência de caracteres de consulta e fragmento.

As cadeias de caracteres de consulta são precedidas por um caractere “?” e normalmente consistem em uma série de pares de nome e valor.

Um fragmento é precedido por um caractere "*#*". Refere-se a uma parte subordinada do recurso que é solicitado na URL.

As partes de uma URL HTTP são mostradas na figura abaixo:

Figura 1.9 Detalha do endereço HTTP



Fonte: CCNA Cyber OPS Associate v1, 2020.

HTTP é um protocolo de solicitação/resposta que usa a porta TCP 80. Ele é flexível, mas não um protocolo seguro.

Quando um cliente envia uma solicitação para um servidor web, ele usará um dos seis métodos especificados por HTTP:

- GET
- POST
- PUT
- DELETE
- OPTIONS
- CONNECT

Códigos de status HTTP

Os códigos de status HTTP são numéricos, com o primeiro número no código indicando o tipo de mensagem.

Os cinco grupos de códigos de status são 1xx- Informativo, 2xx- Sucesso, 3xx- Redirecionamento, 4xx- Erro de cliente e 5xx- Erro de servidor

HTTP/2

O objetivo do HTTP/2 é melhorar o desempenho HTTP abordando problemas de latência que existiam na versão HTTP 1.1 do protocolo.

HTTP/2 usa o mesmo formato de cabeçalho que HTTP 1.1 e usa os mesmos códigos de status.

Alguns recursos importantes do HTTP/2 que um analista de segurança cibernética deve estar ciente:

- Multiplexação
- PUSH do servidor
- Um protocolo binário
- Compressão de cabeçalho

Protegendo HTTP — HTTPS

Para comunicação segura na Internet, é usado o protocolo HTTP Secure (HTTPS).

HTTPS usa autenticação e criptografia para proteger os dados enquanto eles trafegam entre o cliente e o servidor.

HTTPS usa o mesmo processo de resposta do servidor de solicitação do cliente que o HTTP, mas o fluxo de dados é criptografado com Secure Socket Layer (SSL) ou Transport Layer Security (TLS), antes de ser transportado pela rede.

HTTPS/2 é especificado para usar HTTPS sobre TLS com a extensão Application-Layer Protocol Negociation (ALPN) para TLS 1.2 ou mais recente.

Informações confidenciais são transmitidas pela Internet usando HTTPS.

1.3.6 Serviços de transferência e compartilhamento de arquivos

FTP e TFTP

O FTP permite a transferência de dados entre um cliente e um servidor.

Um cliente FTP é executado em um computador e é usado para enviar e receber dados de um servidor FTP.

Conexões FTP entre o cliente e o servidor:

Conexão de controle: O cliente abre a primeira conexão com o servidor para controlar o tráfego.

Conexão de dados: O cliente abre a segunda conexão com o servidor para tráfego de dados.

O Protocolo de Transferência de Ficheiros Trivial (TFTP) é um protocolo de transferência de ficheiros simplificado que utiliza o conhecido número de porta UDP 69.

SMB

O Server Message Block (SMB) é um protocolo de compartilhamento de arquivo cliente / servidor que descreve a estrutura de recursos de rede compartilhados.

SMB é um cliente / servidor, protocolo de solicitação-resposta.

Os servidores podem disponibilizar seus próprios recursos para os clientes na rede.

As mensagens SMB podem iniciar, autenticar e encerrar sessões, controlar o acesso a arquivos e impressoras e permitir que um aplicativo envie ou receba mensagens de ou para outro dispositivo.

O compartilhamento de arquivos SMB e os serviços de impressão se tornaram a base da rede da Microsoft.

Um arquivo pode ser copiado de um computador para outro com o Windows Explorer usando o protocolo SMB.

Conclusão

Concluímos que a camada de transporte é essencial para garantir a entrega adequada dos dados nas redes. A comunicação sem fio, por sua vez, é cada vez mais comum e relevante. Além disso, reforçamos a necessidade de manter a segurança nas infraestruturas de rede.

Referências

Cisco Systems. **Cisco Networking Academy Program CCNA CyberOps Associate** v1, 2020. Disponível em <https://www.netacad.com>.

SÊMOLA, Marcos**. Gestão da segurança da informação**. Rio de Janeiro: Campus, 2003.

NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

THOMAS, Tom. **Segurança de redes**: primeiros passos. Tradução de Flávio MORGADO. Rio de Janeiro: Ciência Moderna, 2007.

BEAL, A. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

STALLINGS, W. **Network security**: applications and standards. 3.nd. New Jersey: Prentice Hall, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001 E 27002**: Tecnologia da informação.

WADLOW, Thomas A. **Segurança de redes**: projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2000.