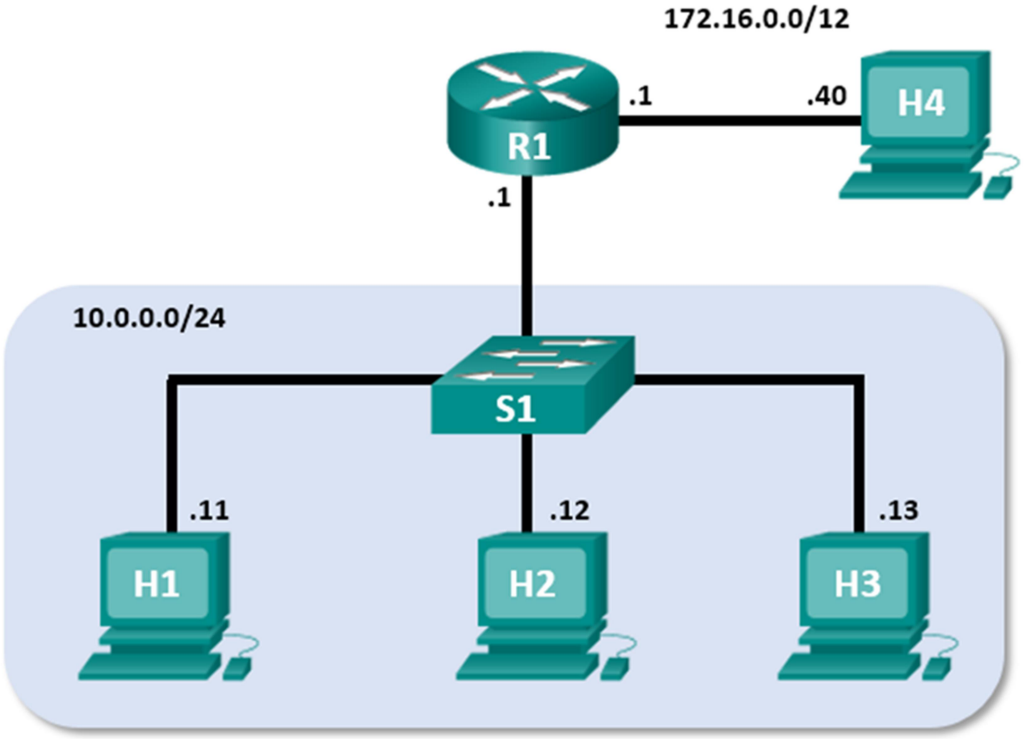
Laboratório – Usando Wireshark para Examinar Quadros Ethernet

Topologia Mininet



Objetivos

Parte 1: Examinar os campos do cabeçalho de um quadro Ethernet II

Parte 2: Usar o Wireshark para capturar e analisar quadros Ethernet

Histórico/Cenário

Quando os protocolos da camada superior se comunicam uns com os outros, os dados fluem para baixo pelas camadas OSI (Open Systems Interconnection) e são encapsulados dentro de um quadro da Camada 2. A composição do quadro depende do tipo de acesso ao meio. Por exemplo, se os protocolos de camada superior forem TCP/IP e o acesso ao meio for Ethernet, o encapsulamento do quadro da Camada 2 será Ethernet II. Isso é comum em um ambiente de LAN.

Ao estudar os conceitos da Camada 2, vale a pena analisar as informações do cabeçalho do quadro. Na primeira parte deste laboratório, você examinará os campos contidos em um quadro Ethernet II. Na Parte 2, você usará o Wireshark para capturar e analisar os campos do cabeçalho de quadros Ethernet II para tráfego local e remoto.

Recursos necessários

- Máquina virtual CyberOps Workstation

Instruções

Parte 1: Examinar os Campos do Cabeçalho de um Quadro Ethernet II

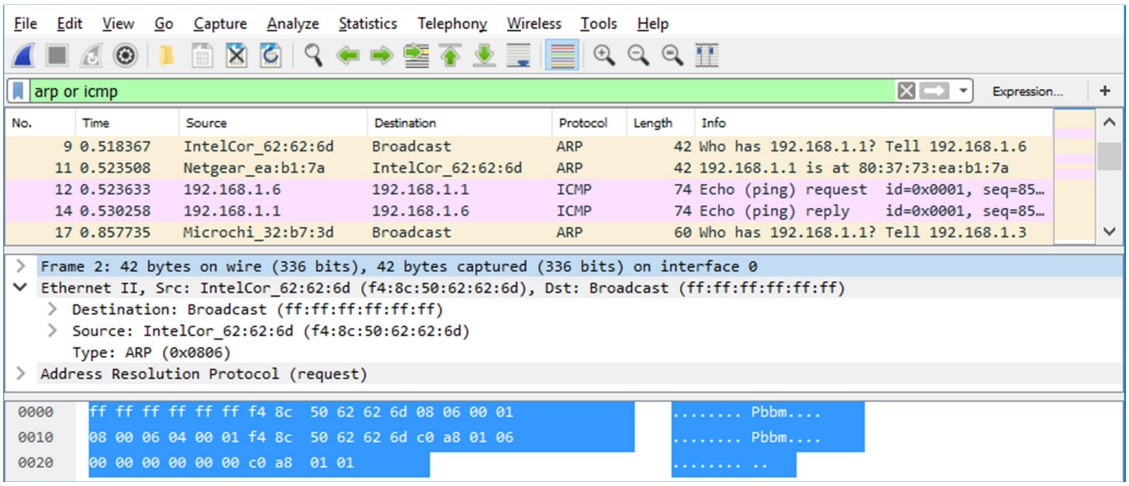
Na Parte 1, você examinará os campos de cabeçalho e o conteúdo em um Quadro Ethernet II fornecido a você. Será usada uma captura do Wireshark para examinar o conteúdo nesses campos.

Etapa 1: Analise os tamanhos e as descrições dos campos do cabeçalho Ethernet II.

Introdução	Endereço de destino	Endereço de Origem	Tipo de moldura	Dados	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1.500 bytes	4 bytes

Etapa 2: Examine os quadros Ethernet em uma captura do Wireshark.

A captura do Wireshark a seguir mostra os pacotes gerados por um ping sendo enviados de um host PC para o gateway padrão. Um filtro foi aplicado ao Wireshark para visualizar somente os protocolos ARP e ICMP. A sessão começa com uma consulta ARP para o endereço MAC do roteador gateway, seguida de quatro requisições e respostas de ping.



Etapa 3: Examine o conteúdo do cabeçalho Ethernet II de uma requisição ARP.

A tabela a seguir usa o primeiro quadro na captura do Wireshark e exibe os dados nos campos do cabeçalho Ethernet II.

Campo	Valor	Descrição
Preâmbulo	Não mostrado na captura	Este campo contém bits de sincronização, processados pelo hardware da NIC.

Campo	Valor	Descrição
Endereço Destino Endereço Origem	Broadcast (ff:ff:ff:ff:ff:ff) IntelCor_62:62:6d (f4:8c:50:62:62:6d)	Endereços de Camada 2 para o quadro. Cada endereço tem 48 bits (ou 6 octetos), expressos como 12 dígitos hexadecimais, `0-9,A-F`. Um formato comum é `12:34:56:78:9A:BC`. Os primeiros seis números hexadecimais indicam o fabricante da placa de interface de rede (NIC) e os últimos seis números hexadecimais são o número de série dela. O endereço destino pode ser broadcast, que contém todos os valores em 1, ou unicast. O endereço origem é sempre unicast.
Tipo de quadro	0x0806	Nos quadros Ethernet II, este campo contém um valor hexadecimal que é usado para indicar o tipo de protocolo de camada superior no campo de dados. Há muitos protocolos de camadas superiores compatíveis com Ethernet II. Dois tipos de quadro comum são: Valor Descrição Protocolo IPv4`0x0800` `0x0806` Protocolo de Resolução de Endereço (ARP)
Dados	ARP	Contém o protocolo de nível superior encapsulado. O campo de dados varia de 46 a 1.500 bytes.
FCS	Não mostrado na captura	Sequência de Verificação de Quadro (FCS), usado pela NIC para identificar erros durante a transmissão. O valor é computado pela máquina emissora, incluindo o endereçamento, o tipo e o campo de dados do quadro. Isso é verificado pelo receptor.

Qual é a importância do conteúdo do campo Endereço Destino?

Por que o PC envia um broadcast ARP antes da primeira requisição ping?

Qual é o endereço MAC origem no primeiro quadro?

Qual é a ID do fornecedor (OUI) da NIC origem?

Que parte do endereço MAC é a OUI?

Qual é o número de série da NIC origem?

Parte 2: Usar o Wireshark para capturar e analisar quadros Ethernet II

Na Parte 2, você usará o Wireshark para capturar quadros Ethernet locais e remotos. Em seguida, examinará as informações contidas nos campos do cabeçalho do quadro.

Etapa 1: Examine a configuração de rede do H3.

a. Inicie e faça login na VM do CyberOps Workstation usando as seguintes credenciais:

Username: **analyst** Password: **cyberops**

b. Abra um emulador de terminal para iniciar o mininet e digite o seguinte comando no prompt. Quando solicitado, digite **cyberops** como a senha.

```
[analista @secOps ~] $ sudo./lab.support.files/scripts/cyberops_topo.py
[sudo] password for analyst:
```

c. No prompt da mininet, inicie as janelas do terminal no host H3.

```
*** Starting CLI:
mininete> xterm H3
```

d. No prompt em Node: h3, digite o **endereço IP** para verificar o endereço IPv4 e registrar o endereço MAC.

Host-interface	Endereço IP	Endereço MAC
H3-eth0		

e. No prompt em Node: H3, digite **netstat -r** para exibir as informações padrão do gateway.

```
[root @secOps ~] # netstat -r
Tabela de roteamento IP do kernel
Destination Gateway Genmask Flags MSS Window irtt Iface
default 10.0.0.1 0.0.0.0 UG 0 0 0 H3-ETH0
10.0.0.0 0.0.0 255.255.255.0 U 0 0 0 H3-ET0
```

Qual é o endereço IP do gateway padrão para o host H3?

Etapa 2: Limpe o cache ARP em H3 e comece a capturar tráfego em H3-eth0.

a. Na janela do terminal de Node: H3, digite **arp -n** para exibir o conteúdo do cache ARP.

```
[root @secOps analista] # arp -n
```

b. Se houver alguma informação ARP existente no cache, limpá-a inserindo o seguinte comando: **arp -d *IP address***. Repita até que todas as informações armazenadas em cache tenham sido limpas.

```
[root@secOps analyst] # arp -n
Endereço HWType HWAddress Flags Mask Iface
10.0.0.11 ether 5a:d 0:1 d: 01:9 f:be C H3-ET0
```

```
[root@secOps analyst] # arp -d 10.0.0.11
Endereço HWType HWAddress Flags Mask Iface
10.0.0.11 (incompleto) C H3-ET0
```

c. Na janela do terminal para Node: H3, abra o Wireshark e inicie uma captura de pacote para a interface H3-eth0.

```
[root@secOps analyst] # wireshark-gtk &
```

Etapa 3: Ping H1 de H3.

a. A partir do terminal em H3, faça ping no gateway padrão e pare depois de enviar 5 pacotes de solicitação de eco.

```
[root@secOps analyst] # ping -c 5 10.0.0.1
```

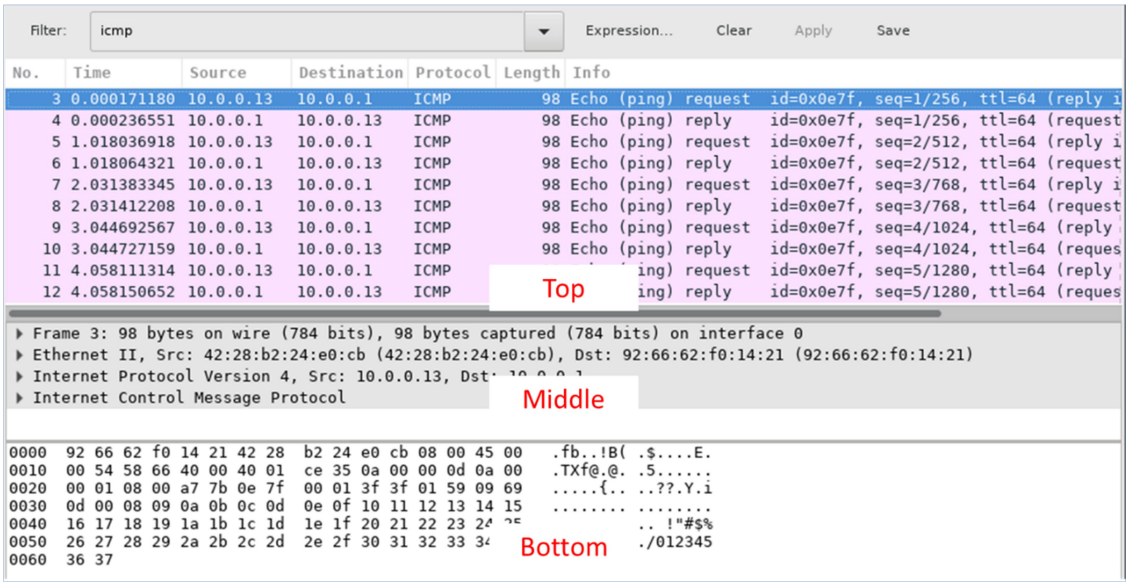
b. Após a conclusão do ping, pare a captura Wireshark.

Etapa 4: Filtrar o Wireshark para exibir apenas o tráfego ICMP.

Aplique o filtro **ICMP** ao tráfego capturado para que apenas o tráfego ICMP seja mostrado nos resultados.

Etapa 5: Examine a primeira requisição (ping) de eco no Wireshark.

A janela principal do Wireshark é dividida em três seções: superior [o painel Packet List (Lista de pacotes)], intermediária [o painel Packet Details (Detalhes do pacote)] e inferior [o painel Packet Bytes (Bytes do pacote)]. Se você tiver selecionado a interface correta para captura de pacotes na Etapa 3, o Wireshark deverá exibir as informações ICMP no painel Packet List (Lista de pacotes), como mostrado no exemplo a seguir.



a. No painel Packet List (Lista de pacotes) [seção superior], clique no primeiro quadro listado. Você deve ver **Echo (ping) request** no cabeçalho **Info (Informações)**. A linha será destacada em azul.

b. Examine a primeira linha no painel Packet Details (Detalhes do pacote) [seção intermediária]. Essa linha apresenta o tamanho do quadro; 98 bytes neste exemplo.

c. A segunda linha no painel Packet Details (Detalhes do pacote) mostra que se trata de um quadro Ethernet II. Os endereços MAC de origem e de destino também são exibidos.

Qual é o endereço MAC da NIC do PC?

Qual é o endereço MAC do gateway padrão?

d. Você pode clicar na seta no início da segunda linha para obter mais informações sobre o quadro Ethernet II.

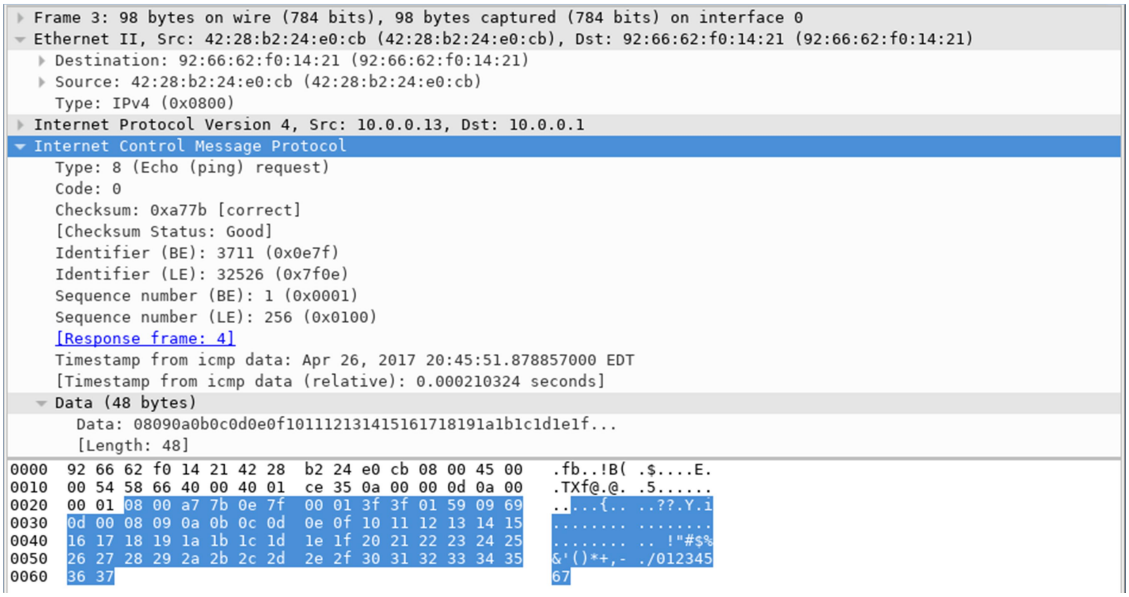
Que tipo de quadro é exibido?

e. As duas últimas linhas exibidas na parte intermediária fornecem informações sobre o campo de dados do quadro. Observe que os dados contêm informações do endereço IPv4 origem e destino.

Qual é o endereço IP de origem?

Qual é o endereço IP de destino?

f. Clique em qualquer linha na seção intermediária para destacar a parte do quadro (hexadecimal e ASCII) no painel Packet Bytes (Bytes do pacote) [seção inferior]. Clique na linha **Internet Control Message Protocol** na seção do meio e examine o que está destacado no painel Packet Bytes.



g. Clique no próximo quadro na seção superior e examine um quadro de resposta de eco. Observe que os endereços MAC de origem e de destino foram invertidos porque esse quadro foi enviado do roteador gateway padrão como uma resposta ao primeiro ping.

   Que dispositivo e endereço MAC são exibidos como endereço destino?

Etapa 6: Inicie uma nova captura no Wireshark.

a. Clique no ícone **Start Capture (Iniciar captura)** para iniciar uma nova captura do Wireshark. Você receberá uma janela pop-up perguntando se deseja salvar os pacotes capturados em um arquivo antes de iniciar uma nova captura. Clique em **Continue without Saving** (Continuar sem salvar).

b. Na janela de terminal de Node: H3, envie 5 pacotes de solicitação de eco para 172.16.0.40.

c. Pare de capturar pacotes quando os pings forem concluídos.

Etapa 7: Examinar os novos dados no painel lista de pacotes do Wireshark.

No primeiro quadro de requisição (ping) de eco, quais são os endereços MAC de origem e de destino?

Fonte:

Destino:

Quais são os endereços IP origem e destino contidos no campo de dados do quadro?

Fonte:

Destino:

Compare esses endereços com os endereços que você recebeu na Etapa 5. O único endereço que mudou foi o endereço IP de destino.

Por que o endereço IP de destino mudou e o endereço MAC de destino permaneceu o mesmo?

Reflexão

O Wireshark não exibe o campo Preâmbulo de um cabeçalho do quadro. O que o preâmbulo contém?