Laboratório 7.5.2: Verificação de Quadro

Diagrama de Topologia

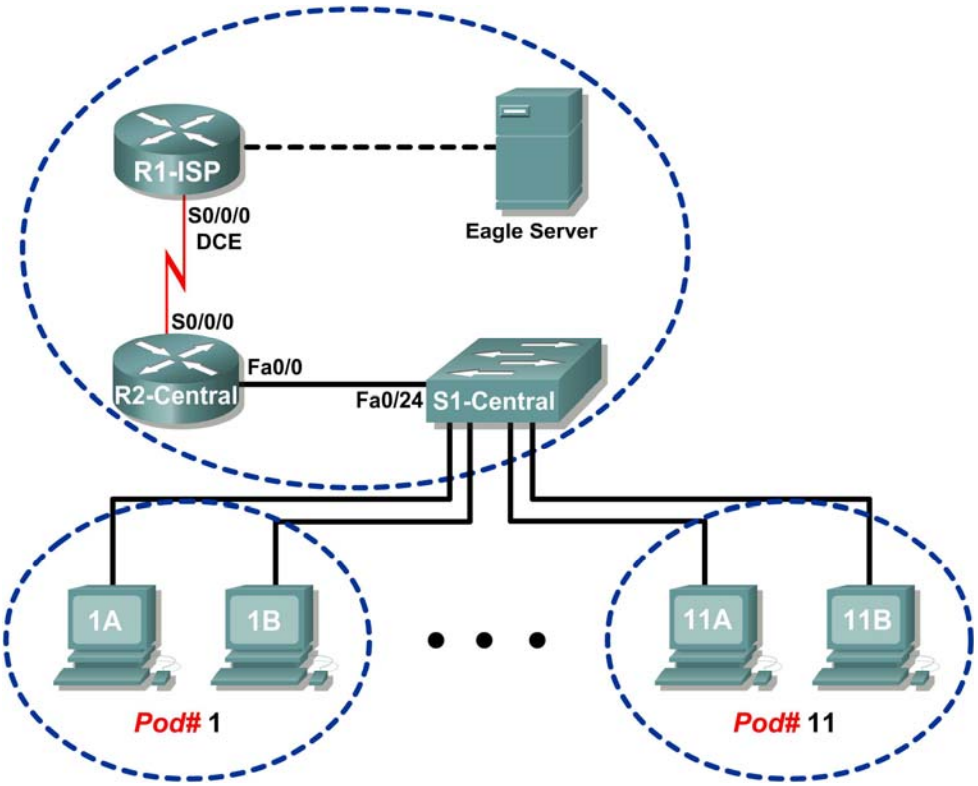

Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway Padrão
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	*N/A*
	Fa0/0	192.168.254.253	255.255.255.0	*N/A*
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	*N/A*
	Fa0/0	172.16.255.254	255.255.0.0	*N/A*
Eagle Server	*N/A*	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.24.254	255.255.255.0	*N/A*
host*Pod#*A	*N/A*	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#*B	*N/A*	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	*N/A*	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos

Com a conclusão deste laboratório, você será capaz de:

- Explicar os campos do cabeçalho em um quadro Ethernet II.
- Usar o Wireshark para capturar e analisar quadros Ethernet II.

Contexto

Quando os protocolos da camada superior comunicam uns com os outros, os dados fluem para as camadas OSI e são encapsulados dentro de um quadro da Camada 2. A composição do quadro depende do tipo de acesso da mídia. Por exemplo, se o protocolo de camada superior é o TCP/IP e a meio de acesso é Ethernet, então o encapsulamento do quadro da Camada 2 será em Ethernet II.

No estudo dos conceitos da Camada 2, deve-se analisar a informação do cabeçalho do quadro. O cabeçalho do quadro Ethernet II será examinado neste laboratório. Quadros Ethernet II podem suportar vários protocolos de camadas superiores, como o TCP/IP.

Cenário

O Wireshark será usado para capturar e analisar os campos do cabeçalho do quadro Ethernet II. Se o Wireshark não foi instalado no computador, ele pode ser baixado da URL `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter7/`, arquivo `wireshark-setup-0.99.4.exe`.

O comando **`ping`** do Windows será usado para gerar tráfego de rede para o Wireshark capturar.

Tarefa 1: Explique os campos do cabeçalho de um quadro Ethernet II

O formato para um quadro Ethernet II é o na figura 1.

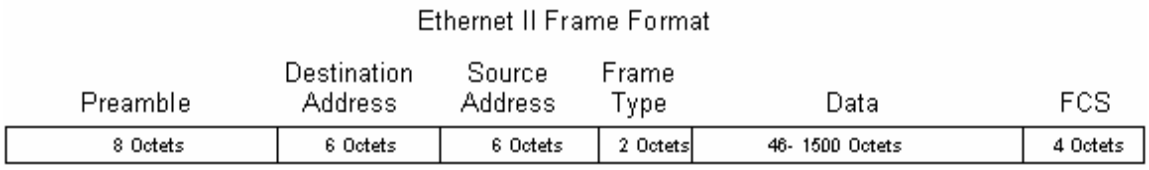

Figura 1. Formato do Quadro Ethernet II

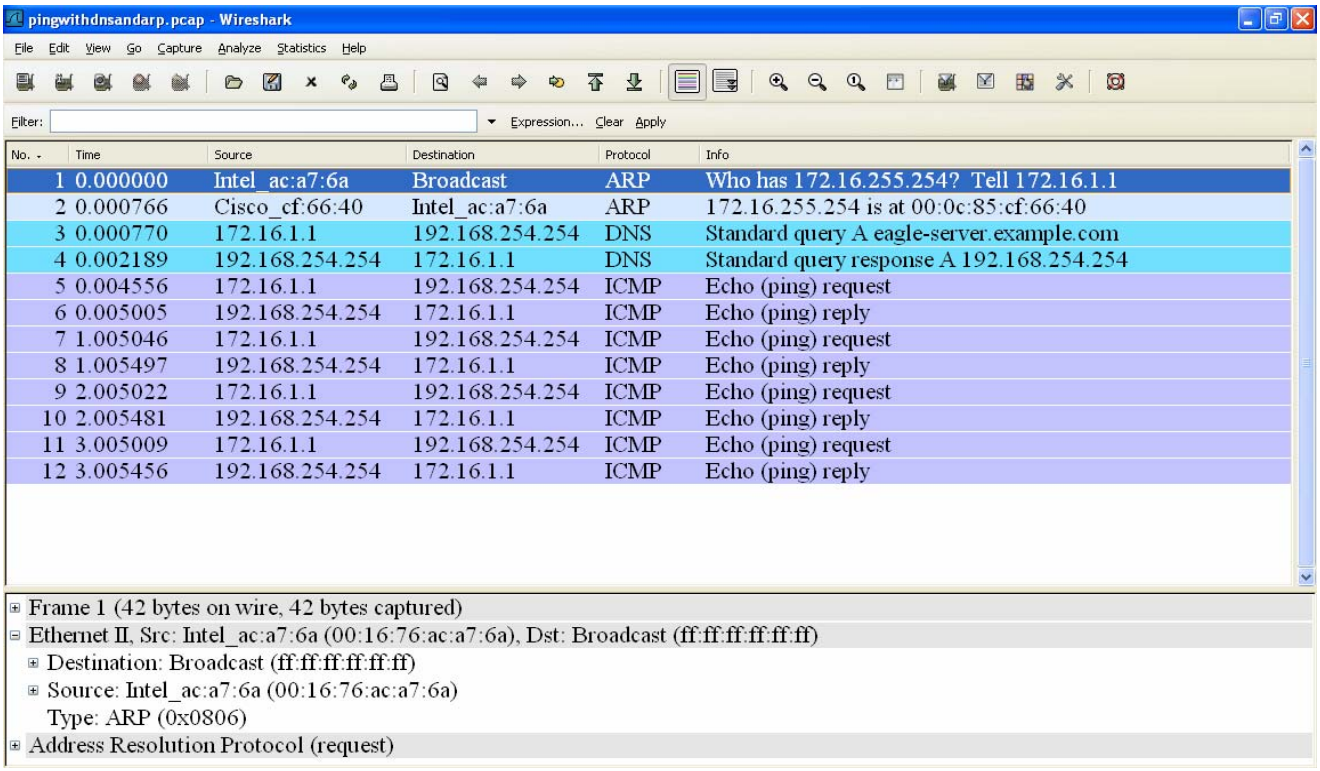

Figura 2. Captura pelo Wireshark do Comando `ping`

Na Figura 2, a janela Panel List mostra uma captura pelo Wireshark do comando **`ping`** entre o computador e o Eagle Server. A sessão começa com o protocolo ARP solicitando o endereço MAC da Porta do roteador, seguido por uma consulta DNS. Finalmente, o comando **`ping`** envia solicitações de echo.

Na Figura 2, a janela Detalhes do Pacote mostra as informações de detalhes do Quadro 1. Usando esta janela, as seguintes informações do quadro da Ethernet II podem ser obtidas:

Campo	Valor	Descrição
Preâmbulo	Não o na captura	Este campo contém bits sincronizados, processados pelo hardware da NIC.
Endereço de Destino	`ff:ff:ff:ff:ff:ff`	00:16:76:ac:a7:6a Cada endereço tem o tamanho de 48 bits, ou 6 bytes, descritos como 12 dígitos hexadecimais, `0-9,A-F`. Um formato comum é `12:34:56:78:9A:BC`. 0x0806 Veja http://www.neotechcc.org/forum/macid.htm para a lista de códigos de vendedores. Os últimos seis dígitos hexadecimais, `ac:a7:6a`, são o número serial do NIC. O endereço de destino pode ser um broadcast que contém todos `1s` ou unicast. Dois tipos de frame comum são:
Endereço de Origem	`00:16:76:ac:a7:6a`	
Tipo de Quadro	`0x0806`	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 suportados pelo Ethernet

Campo	Valor	Descrição
		II. Dois tipos de quadro comum são: Valor Descrição 0x0800 Protocolo IPv4 0x0806 Resolução de Endereço O valor é computado pela máquina emissora, incluindo endereços de frame, tipo e campo de dados.
Dados	ARP	Contém o protocolo de nível superior encapsulado. O campo de dados é entre 46 – 1500 bytes.
FCS	Não o na captura	Seqüência de Verificação do Quadro , usado pela NIC para identificar erros durante a transmissão. O valor é computado pela máquina emissora, incluindo endereços do quadro, tipo e campo de dados. Isso é verificado pelo receptor.

Qual é o significado de todos os **1**s no campo de endereço de destino?

_____

_____

A partir da informação contida na janela do Packet List para o **primeiro** quadro, responda as seguintes perguntas sobre o endereço MAC de destino e de origem:

Endereço de Destino:

Endereço MAC : _____
Fabricante NIC : _____
Número de Série NIC: _____

Endereço de Origem:

Endereço MAC : _____
Fabricante NIC : _____
Número de Série NIC: _____

A partir da informação contida na janela do Packet List para o **segundo** quadro, responda as seguintes perguntas sobre o endereço MAC de destino e de origem:

Endereço de Destino:

Endereço MAC : _____
Fabricante NIC : _____
Número de Série NIC: _____

Endereço de Origem:

Endereço MAC : _____
Fabricante NIC : _____
Número de Série NIC: _____

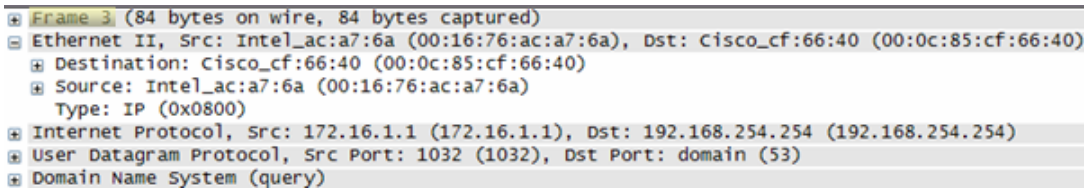

Figura 3. Campos do Quadro 3

A Figura 3 contém uma visão expandida da captura do Quadro 3 pelo Wireshark. Use a informação para completar a seguinte tabela:

Campo	Valor
Preâmbulo	
Endereço de Destino	
Endereço de Origem	
Tipo de Quadro	
Dados	
FCS	

Na seguinte tarefa, o Wireshark será usado para capturar e analisar pacotes capturados no computador.

Tarefa 2: Use o Wireshark para Capturar e analisar Quadros Ethernet II

Passo 1: Configure o Wireshark para capturas de pacote.

Prepare o Wireshark para capturas. Clique em **Capture > Interfaces**, e depois clique no botão de início que corresponde ao endereço IP da interface 172.16.x.y . Isto iniciará a captura do pacote.

Passo 2: Inicie um ping para o Eagle Server e capture a sessão.

Abra uma janela de terminal do Windows. Clique em **Start > Run**, digite **cmd**, e clique **OK**.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\> ping eagle-server.example.com

Pinging eagle-server.example.com [192.168.254.254] with 32 bytes of
data:

Reply from 192.168.254.254: bytes=32 time<1ms TTL=62
Reply from 192.168.254.254: bytes=32 time<1ms TTL=62
Reply from 192.168.254.254: bytes=32 time<1ms TTL=62
Reply from 192.168.254.254: bytes=32 time<1ms TTL=62

Ping statistics for 192.168.254.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\ >
```

Figura 4. Ping para eagle-server.example.com

Execute Ping no eagle-server.example.com, conforme o na Figura 4. Quando o comando finaliza a execução, pare as capturas do Wireshark.

Passo 3: Analise a captura do Wireshark.

A janela Packet List do Wireshark deve iniciar com uma solicitação e resposta ARP para o endereço MAC da Porta de Conexão. Em seguida, um pedido de DNS é feito para o endereço IP do eagle-server.example.com. Finalmente, o comando **`ping`** é executado. Sua captura deve mostrar-se parecida com a na Figura 2.

Use sua captura do Wireshark do comando **`ping`** para responder as seguintes questões:

Informação do endereço MAC do computador pod:

Endereço MAC : _____

Fabricante NIC : _____

Número de Série NIC: _____

Informação do endereço MAC do R2-Central:

Endereço MAC : _____

Fabricante NIC : _____

Número de Série NIC: _____

Um aluno de outra escola gostaria de saber o endereço MAC para o Eagle Server. O que você diria ao aluno?

Qual é o valor do campo tipo de quadro Ethernet II para uma Solicitação ARP?

_____

Qual é o valor do campo tipo de quadro Ethernet II para uma Resposta ARP ?

_____

Qual é o valor do campo tipo de quadro Ethernet II para uma consulta DNS ?

_____

Qual é o valor do campo tipo de quadro Ethernet II para uma resposta de consulta DNS ?

_____

Qual é o valor do campo tipo de quadro Ethernet II para um echo ICMP?

_____

Qual é o valor do campo tipo de quadro Ethernet II para uma resposta de echo ICMP?

_____

Tarefa 3: Desafio

Use o Wireshark para capturar sessões de outros protocolos TCP/IP, tais como FTP e HTTP. Analise os pacotes capturados, e verifique que o tipo de quadro Ethernet II permanece com o valor `0x0800`.

Tarefa 4: Reflexão

Neste laboratório, a informação do cabeçalho do quadro Ethernet II foi examinada. Um campo de preâmbulo contém sete bytes de seqüências `0101` alternadas, e um byte que sinaliza o início do quadro, `01010110`. Endereços MAC de destino e de origem contêm 12 dígitos hexa. Os primeiros seis dígitos

hexa contêm o fabricante da NIC, e os últimos seis dígitos hexa contêm o número de série da NIC. Se o quadro é um broadcast, o endereço MAC de destino contém somente bits1. Um campo tipo de quadro de 4-byte contém um valor que indica o protocolo no campo dados. Para IPv4, o valor é `0x0800.` O campo dados é variável e contém o protocolo de camada superior encapsulado. No final de um quadro, um valor FCS de 4-byte é usado para verificar que não existiram erros durante a transmissão.

Tarefa 5: Limpeza

O Wireshark foi instalado no computador. Se o Wireshark precisar ser desinstalado, clique em **Iniciar> Painel de Controle.** Abra **Adicionar ou Remover Programas**. Selecione o Wireshark, e clique em **Remover**.

Remova quaisquer arquivos criados no computador durante o laboratório.

A menos que não solicitado pelo instrutor, desligue os computadores. Remova qualquer coisa que tenha sido trazida ao laboratório e deixe a sala pronta para a próxima aula.

