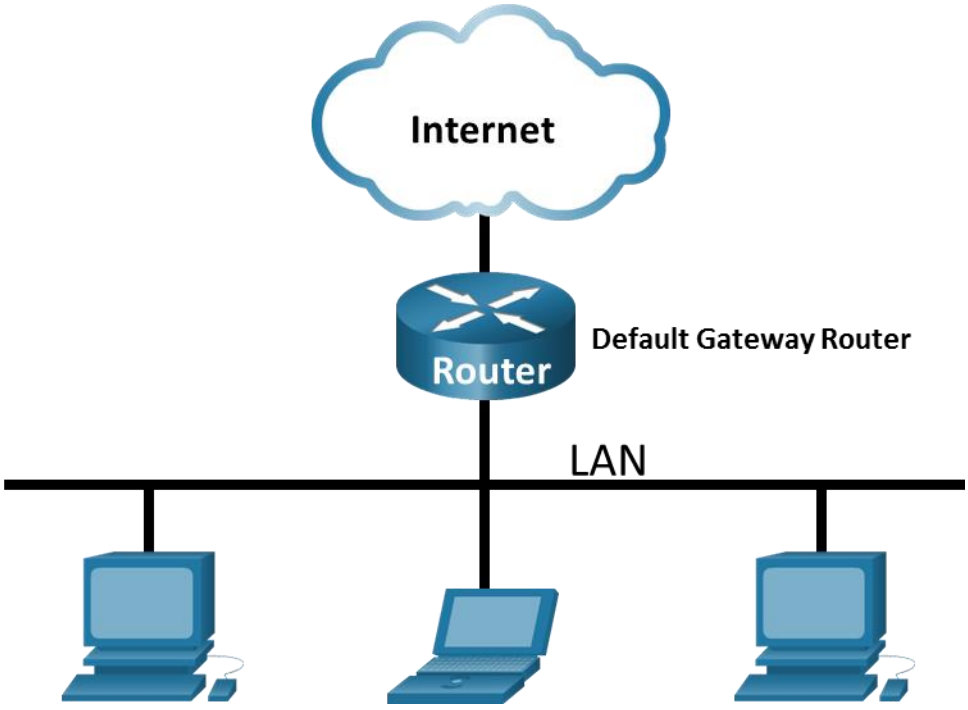
Laboratorio - Utilizzo di Wireshark per la visualizzazione del traffico di rete

Topologia



Obiettivi

Parte 1: Acquisire e analizzare i dati ICMP locali in Wireshark

Parte 2: Acquisire e analizzare i dati ICMP remoti in Wireshark

Introduzione e scenario

Wireshark è un analizzatore software di protocolli (applicazione “packet sniffer”) utilizzato per la risoluzione dei problemi di rete, lo sviluppo di software e protocolli e l'apprendimento. Quando i flussi di dati viaggiano continuamente avanti e indietro nella rete, lo sniffer “cattura” tutte le Protocol Data Unit (PDU) ed è in grado di decodificarne e analizzarne i contenuti in base all'RFC appropriato o ad altre specifiche.

Wireshark è uno strumento utile per chiunque utilizzi le reti e può essere utilizzato nella maggior parte delle attività di laboratorio dei corsi CCNA per l'analisi dei dati e la risoluzione dei problemi. In questa attività di laboratorio, si utilizzerà Wireshark per acquisire gli indirizzi IP dei pacchetti di dati ICMP e gli indirizzi MAC del frame Ethernet.

Risorse necessarie

- 1 PC (Windowscon accesso a internet)
- Verranno utilizzati ulteriori computer nella rete locale (LAN) per rispondere alle richieste ping.

Istruzioni

Parte 1: Acquisizione e analisi dei dati ICMP locali in Wireshark

Nella Parte 1 di questa attività di laboratorio, si eseguirà il ping a un altro computer sulla LAN e si acquisiranno le richieste e le risposte ICMP in Wireshark. Inoltre, si esamineranno i frame acquisiti per rilevare informazioni specifiche. Questa analisi contribuirà a chiarire il modo in cui gli header dei pacchetti vengono utilizzati per trasportare dati alla destinazione.

Fase 1: Recuperare gli indirizzi dell'interfaccia del computer.

Per questa attività di laboratorio, è necessario recuperare l'indirizzo IP del computer e il relativo indirizzo fisico della scheda di rete (Network Interface Card - NIC), detto anche indirizzo MAC.

a. In una finestra del prompt dei comandi, immettere **ipconfig /all**, all'indirizzo IP dell'interfaccia PC, alla sua descrizione e al suo indirizzo MAC (fisico).

```
C:\Users\Student> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC
   Primary Dns Suffix . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . :00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
<output omitted>
```

b. Chiedere a un membro(i) del team l'indirizzo IP del suo PC e fornire l'indirizzo IP del proprio PC ma non scambiare l'indirizzo MAC.

Fase 2: Avviare Wireshark e iniziare ad acquisire dati.

a. Vai a Wireshark. Fare doppio clic sull'interfaccia desiderata per avviare l'acquisizione dei pacchetti. Assicurarsi che l'interfaccia desiderata abbia traffico.

b. Le informazioni iniziano a scorrere verso il basso dalla sezione superiore in Wireshark. Le righe di dati vengono visualizzate con colori diversi a seconda del protocollo.

Queste informazioni possono scorrere molto rapidamente a seconda della comunicazione in corso tra il computer e la LAN. È possibile applicare un filtro per semplificare la visualizzazione e l'utilizzo dei dati acquisiti da Wireshark.

In questa attività di laboratorio si intende visualizzare solo le PDU del protocollo ICMP (ping). Digitare **icmp** nella casella **Filter** nella parte superiore di Wireshark e premere **Invio,** o fare clic su **Apply** (freccia) per visualizzare solo le PDU del protocollo ICMP (ping).

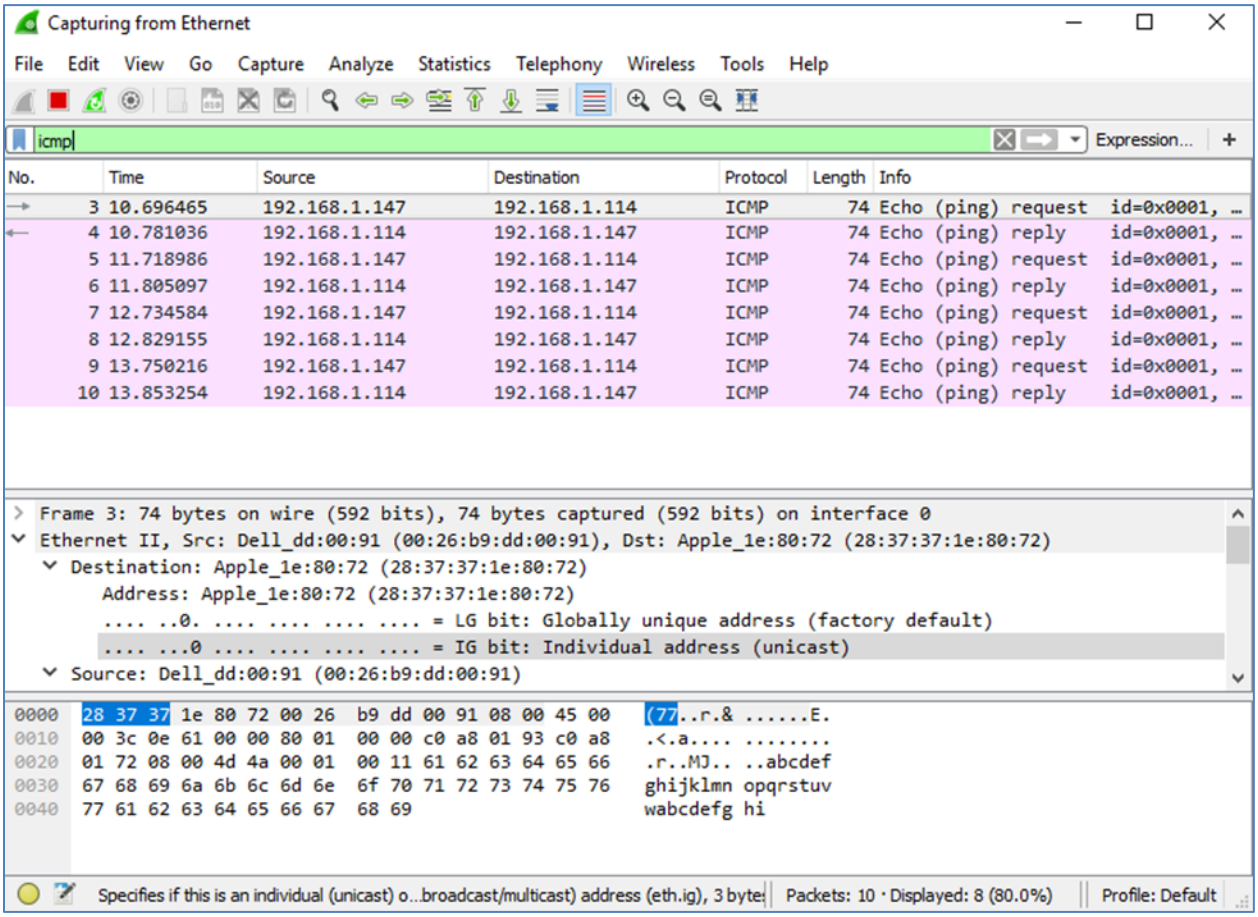
c. Questo filtro fa scomparire tutti i dati nella finestra superiore, ma il traffico continua a essere acquisito sull'interfaccia. Passare a una finestra del prompt dei comandi e eseguire il ping dell'indirizzo IP ricevuto dal membro del team.

```
C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Notare che i dati iniziano a comparire nuovamente nella finestra superiore di Wireshark.



Nota: Se il PC del membro del team non risponde ai tuoi ping, è possibile che il firewall del PC del membro del team stia bloccando queste richieste. Vedere Appendice A: Passaggio del traffico ICMP attraverso un firewall per informazioni su come consentire il traffico ICMP attraverso il firewall utilizzando Windows.

d. Arrestare l'acquisizione dei dati facendo clic sull'icona **Stop capture**.

Fase 3: Esaminare i dati acquisiti.

Nella Fase 3, esaminare i dati generati dalle richieste di ping del computer del membro del team. I dati di Wireshark vengono visualizzati in tre sezioni: 1) la sezione superiore visualizza l'elenco dei frame PDU acquisiti, insieme a un elenco riepilogativo delle informazioni dei pacchetti IP, 2) la sezione centrale elenca le informazioni sulle PDU per il frame selezionato nella parte superiore della schermata e separa un frame PDU acquisito nei suoi livelli protocollari e 3) la sezione inferiore visualizza i dati non elaborati di ogni livello. I dati non elaborati vengono visualizzati in formato sia esadecimale che decimale.

a. Fare clic sui primi frame PDU della richiesta ICMP nella sezione superiore di Wireshark. Notare che la colonna **Source** contiene l'indirizzo IP del computer, mentre la colonna **Destination** contiene l'indirizzo IP del computer del membro del team al quale è stato inviato il ping.

b. Con questo frame PDU ancora selezionato nella sezione superiore, accedere alla sezione centrale. Fare clic sul segno più a sinistra della riga Ethernet II per visualizzare la destinazione e gli indirizzi MAC di origine.

L'indirizzo MAC di origine corrisponde all'interfaccia del computer?

L'indirizzo MAC di destinazione in Wireshark corrisponde all'indirizzo MAC del membro del team?

Come viene ottenuto l'indirizzo MAC del computer al quale è stato inviato il ping da parte del proprio computer?

Nota: Nell'esempio precedente di una richiesta ICMP acquisita, i dati ICMP sono incapsulati in una PDU del pacchetto IPv4 (header IPv4), che a sua volta è incapsulata in una PDU del frame Ethernet II (header Ethernet II) per la trasmissione nella LAN.

Parte 2: Acquisizione e analisi dei dati ICMP remoti in Wireshark

Nella Parte 2 verrà eseguito il ping degli host remoti (host non presenti sulla LAN) e verranno esaminati i dati generati da questi ping. Si stabilirà quindi la differenza tra questi dati e i dati esaminati nella Parte 1.

Fase 1: Avviare l'acquisizione dei dati sull'interfaccia.

a. Avviare di nuovo l'acquisizione dei dati.

b. Una finestra chiede di salvare i dati precedentemente acquisiti prima di iniziare un'altra acquisizione. Non è necessario salvare questi dati. Fare clic su **Continue without Saving**.

c. Con l'acquisizione attiva, eseguire il ping dei seguenti tre URL del sito web da un prompt dei comandi di Windows:

1) www.yahoo.com
2) www.cisco.com
3) www.google.com

Nota: Quando si esegue il ping degli URL indicati, notare che il DNS (Domain Name Server) converte l'URL in un indirizzo IP. Prendere nota dell'indirizzo IP ricevuto per ogni URL.

d. È possibile arrestare l'acquisizione dei dati facendo clic sull'icona **Stop Capture**.

Fase 2: Esame e analisi dei dati provenienti dagli host remoti.

Rivedere i dati acquisiti in Wireshark ed esaminare gli indirizzi IP e MAC delle tre posizioni alle quali sono stati inviati i ping. Elencare gli indirizzi IP e MAC di destinazione di tutte e tre le posizioni nello spazio fornito.

Indirizzo IP per **www.yahoo.com**:

Indirizzo MAC per **www.yahoo.com**:

Indirizzo IP per **www.cisco.com**:

Indirizzo MAC per **www.cisco.com**:

Indirizzo IP per **www.google.com**:

Indirizzo MAC per **www.google.com**:

Cosa è importante osservare in queste informazioni?

Qual è la differenza tra queste informazioni e le informazioni del ping locale ricevute nella Parte 1?

Domande di riflessione

Perché Wireshark mostra l'indirizzo MAC effettivo degli host locali, ma non l'indirizzo MAC effettivo degli host remoti?

Appendice A: Passaggio del traffico ICMP attraverso un firewall

Se i membri del team non sono in grado di eseguire il ping del computer, è probabile che il firewall stia bloccando tali richieste. In questa appendice viene illustrata la modalità di creazione di una regola nel firewall per consentire le richieste ping. Inoltre, viene descritta la modalità di disattivazione della nuova regola ICMP dopo il completamento del laboratorio.

Parte 1: Creare una nuova regola in entrata consentendo il passaggio del traffico ICMP attraverso il firewall.

a. Passare al **Pannello di controllo** e fare clic sull'opzione **Sistema e sicurezza** nella visualizzazione Categoria.

b. Nella finestra **Sistema e sicurezza** fare clic su **Windows Defender Firewall** o **Windows Firewall**.

c. Nel riquadro a sinistra della finestra **Windows Defender Firewall** o **Windows Firewall** fare clic su **Impostazioni avanzate**.

d. Nella finestra **Sicurezza avanzata** selezionare l'opzione **Regole connessioni in entrata** nella barra laterale sinistra, quindi fare clic su **Nuova regola…** nella barra laterale destra.

e. In questo modo viene avviata la creazione guidata **nuova regola connessioni in entrata**. Nella schermata **Tipo di regola**, fare clic sul pulsante di **scelta personalizzata**, quindi su **Avanti**.

f. Nel riquadro a sinistra fare clic su **Protocollo e porte** e, utilizzando il menu a discesa **Tipo di protocollo**, selezionare **ICMPv4**, quindi fare clic su **Avanti**.

g. Verificare che sia selezionato **qualsiasi indirizzo IP** per gli indirizzi IP locali e remoti. Fare clic su **Avanti** per continuare.

h. Selezionare **Consenti la connessione**. Fare clic su **Avanti** per continuare.

i. Per impostazione predefinita, questa regola si applica a tutti i profili. Fare clic su **Avanti** per continuare.

j. Assegnare un nome alla regola con **Consenti richieste ICMP**. Fare clic su **Fine** per continuare. Questa nuova regola consentirà ai membri del team di ricevere risposte ping dal computer.

Parte 2: Disabilitare o eliminare la nuova regola ICMP.

Dopo aver completato l'attività di laboratorio, potrebbe essere opportuno disabilitare o persino eliminare la nuova regola creata nella Fase 1. Utilizzando l'opzione **Disabilita regola** è possibile abilitare nuovamente la regola in un secondo momento. L'eliminazione della regola la elimina in modo permanente dall'elenco delle regole connessioni in entrata.

a. Nella finestra **Sicurezza avanzata** selezionare l'opzione **Regole connessioni in entrata** nel riquadro a sinistra, quindi individuare la regola creata precedentemente.

b. Fare clic con il pulsante destro del mouse sulla regola ICMP e selezionare **Disabilita regola**, se lo si desidera. È inoltre possibile selezionare **Elimina** se si desidera eliminarla definitivamente. Se si sceglie questa opzione, è necessario creare nuovamente la regola per consentire le risposte ICMP.