

- TP4 -

Les objectifs de ce TP sont:

- Etude de de la commande ping avec l'environnement de simulation réseau PacketTracer
- Se familiarisé avec l'environnement du sniffer WIRESHARK
- Analyse des trames dans les réseaux sans fil.

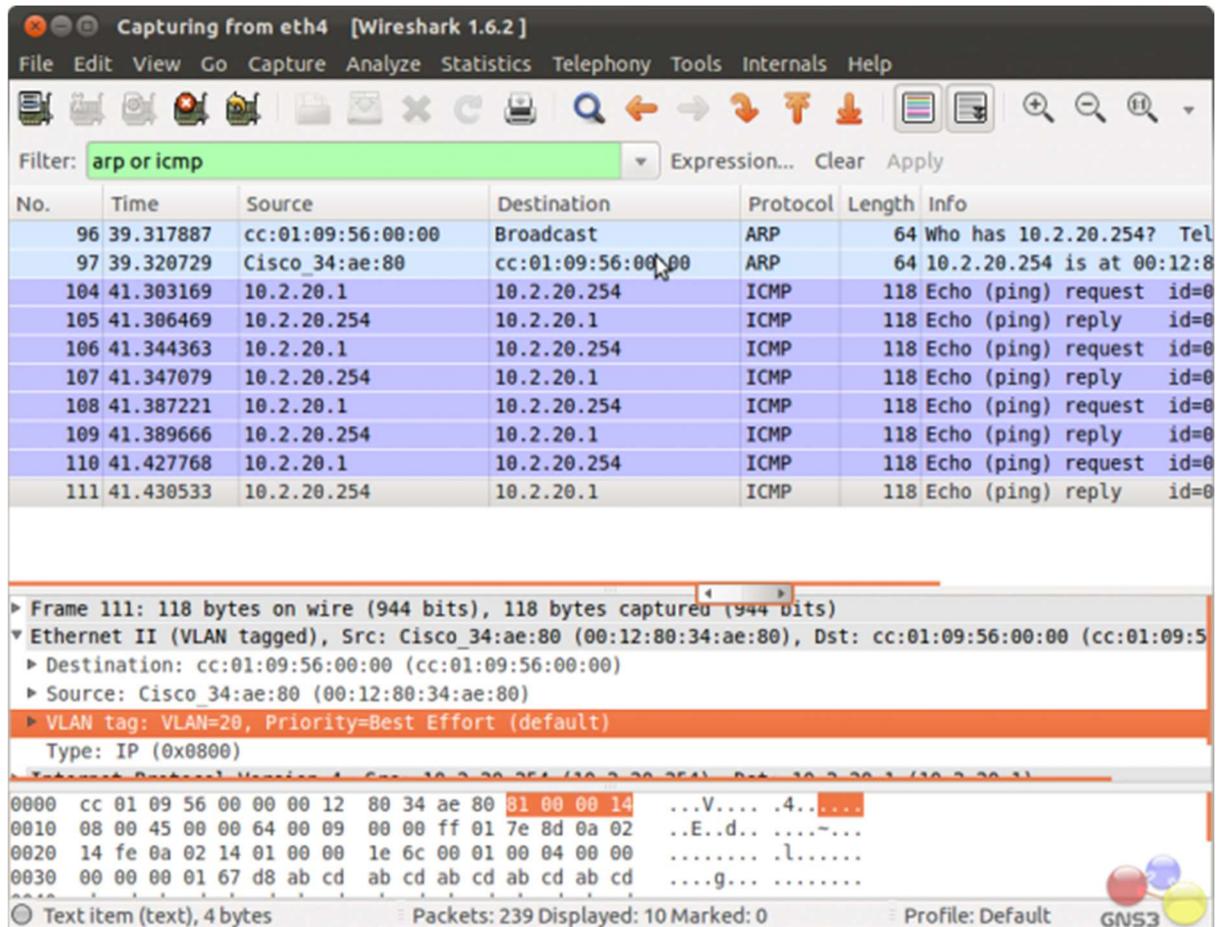
1) Etude des paquets du protocole ICMP sous PacketTracer

The screenshot displays the Packet Tracer interface. The main window shows a logical network with two PCs, PC1 and PC0, connected by a dashed line. A central window titled "PDU Information at Device: PC1" displays the details of an outgoing packet. The packet structure is as follows:

Ethernet II																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
0	14	18	22	26	30	34	38	42	46	50	54	58	62	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126	130	134	138	142	146	150	154	158	162	166	170	174	178	182	186	190	194	198	202	206	210	214	218	222	226	230	234	238	242	246	250	254	258	262	266	270	274	278	282	286	290	294	298	302	306	310	314	318	322	326	330	334	338	342	346	350	354	358	362	366	370	374	378	382	386	390	394	398	402	406	410	414	418	422	426	430	434	438	442	446	450	454	458	462	466	470	474	478	482	486	490	494	498	502	506	510	514	518	522	526	530	534	538	542	546	550	554	558	562	566	570	574	578	582	586	590	594	598	602	606	610	614	618	622	626	630	634	638	642	646	650	654	658	662	666	670	674	678	682	686	690	694	698	702	706	710	714	718	722	726	730	734	738	742	746	750	754	758	762	766	770	774	778	782	786	790	794	798	802	806	810	814	818	822	826	830	834	838	842	846	850	854	858	862	866	870	874	878	882	886	890	894	898	902	906	910	914	918	922	926	930	934	938	942	946	950	954	958	962	966	970	974	978	982	986	990	994	998	1002	1006	1010	1014	1018	1022	1026	1030	1034	1038	1042	1046	1050	1054	1058	1062	1066	1070	1074	1078	1082	1086	1090	1094	1098	1102	1106	1110	1114	1118	1122	1126	1130	1134	1138	1142	1146	1150	1154	1158	1162	1166	1170	1174	1178	1182	1186	1190	1194	1198	1202	1206	1210	1214	1218	1222	1226	1230	1234	1238	1242	1246	1250	1254	1258	1262	1266	1270	1274	1278	1282	1286	1290	1294	1298	1302	1306	1310	1314	1318	1322	1326	1330	1334	1338	1342	1346	1350	1354	1358	1362	1366	1370	1374	1378	1382	1386	1390	1394	1398	1402	1406	1410	1414	1418	1422	1426	1430	1434	1438	1442	1446	1450	1454	1458	1462	1466	1470	1474	1478	1482	1486	1490	1494	1498	1502	1506	1510	1514	1518	1522	1526	1530	1534	1538	1542	1546	1550	1554	1558	1562	1566	1570	1574	1578	1582	1586	1590	1594	1598	1602	1606	1610	1614	1618	1622	1626	1630	1634	1638	1642	1646	1650	1654	1658	1662	1666	1670	1674	1678	1682	1686	1690	1694	1698	1702	1706	1710	1714	1718	1722	1726	1730	1734	1738	1742	1746	1750	1754	1758	1762	1766	1770	1774	1778	1782	1786	1790	1794	1798	1802	1806	1810	1814	1818	1822	1826	1830	1834	1838	1842	1846	1850	1854	1858	1862	1866	1870	1874	1878	1882	1886	1890	1894	1898	1902	1906	1910	1914	1918	1922	1926	1930	1934	1938	1942	1946	1950	1954	1958	1962	1966	1970	1974	1978	1982	1986	1990	1994	1998	2002	2006	2010	2014	2018	2022	2026	2030	2034	2038	2042	2046	2050	2054	2058	2062	2066	2070	2074	2078	2082	2086	2090	2094	2098	2102	2106	2110	2114	2118	2122	2126	2130	2134	2138	2142	2146	2150	2154	2158	2162	2166	2170	2174	2178	2182	2186	2190	2194	2198	2202	2206	2210	2214	2218	2222	2226	2230	2234	2238	2242	2246	2250	2254	2258	2262	2266	2270	2274	2278	2282	2286	2290	2294	2298	2302	2306	2310	2314	2318	2322	2326	2330	2334	2338	2342	2346	2350	2354	2358	2362	2366	2370	2374	2378	2382	2386	2390	2394	2398	2402	2406	2410	2414	2418	2422	2426	2430	2434	2438	2442	2446	2450	2454	2458	2462	2466	2470	2474	2478	2482	2486	2490	2494	2498	2502	2506	2510	2514	2518	2522	2526	2530	2534	2538	2542	2546	2550	2554	2558	2562	2566	2570	2574	2578	2582	2586	2590	2594	2598	2602	2606	2610	2614	2618	2622	2626	2630	2634	2638	2642	2646	2650	2654	2658	2662	2666	2670	2674	2678	2682	2686	2690	2694	2698	2702	2706	2710	2714	2718	2722	2726	2730	2734	2738	2742	2746	2750	2754	2758	2762	2766	2770	2774	2778	2782	2786	2790	2794	2798	2802	2806	2810	2814	2818	2822	2826	2830	2834	2838	2842	2846	2850	2854	2858	2862	2866	2870	2874	2878	2882	2886	2890	2894	2898	2902	2906	2910	2914	2918	2922	2926	2930	2934	2938	2942	2946	2950	2954	2958	2962	2966	2970	2974	2978	2982	2986	2990	2994	2998	3002	3006	3010	3014	3018	3022	3026	3030	3034	3038	3042	3046	3050	3054	3058	3062	3066	3070	3074	3078	3082	3086	3090	3094	3098	3102	3106	3110	3114	3118	3122	3126	3130	3134	3138	3142	3146	3150	3154	3158	3162	3166	3170	3174	3178	3182	3186	3190	3194	3198	3202	3206	3210	3214	3218	3222	3226	3230	3234	3238	3242	3246	3250	3254	3258	3262	3266	3270	3274	3278	3282	3286	3290	3294	3298	3302	3306	3310	3314	3318	3322	3326	3330	3334	3338	3342	3346	3350	3354	3358	3362	3366	3370	3374	3378	3382	3386	3390	3394	3398	3402	3406	3410	3414	3418	3422	3426	3430	3434	3438	3442	3446	3450	3454	3458	3462	3466	3470	3474	3478	3482	3486	3490	3494	3498	3502	3506	3510	3514	3518	3522	3526	3530	3534	3538	3542	3546	3550	3554	3558	3562	3566	3570	3574	3578	3582	3586	3590	3594	3598	3602	3606	3610	3614	3618	3622	3626	3630	3634	3638	3642	3646	3650	3654	3658	3662	3666	3670	3674	3678	3682	3686	3690	3694	3698	3702	3706	3710	3714	3718	3722	3726	3730	3734	3738	3742	3746	3750	3754	3758	3762	3766	3770	3774	3778	3782	3786	3790	3794	3798	3802	3806	3810	3814	3818	3822	3826	3830	3834	3838	3842	3846	3850	3854	3858	3862	3866	3870	3874	3878	3882	3886	3890	3894	3898	3902	3906	3910	3914	3918	3922	3926	3930	3934	3938	3942	3946	3950	3954	3958	3962	3966	3970	3974	3978	3982	3986	3990	3994	3998	4002	4006	4010	4014	4018	4022	4026	4030	4034	4038	4042	4046	4050	4054	4058	4062	4066	4070	4074	4078	4082	4086	4090	4094	4098	4102	4106	4110	4114	4118	4122	4126	4130	4134	4138	4142	4146	4150	4154	4158	4162	4166	4170	4174	4178	4182	4186	4190	4194	4198	4202	4206	4210	4214	4218	4222	4226	4230	4234	4238	4242	4246	4250	4254	4258	4262	4266	4270	4274	4278	4282	4286	4290	4294	4298	4302	4306	4310	4314	4318	4322	4326	4330	4334	4338	4342	4346	4350	4354	4358	4362	4366	4370	4374	4378	4382	4386	4390	4394	4398	4402	4406	4410	4414	4418	4422	4426	4430	4434	4438	4442	4446	4450	4454	4458	4462	4466	4470	4474	4478	4482	4486	4490	4494	4498	4502	4506	4510	4514	4518	4522	4526	4530	4534	4538	4542	4546	4550	4554	4558	4562	4566	4570	4574	4578	4582	4586	4590	4594	4598	4602	4606	4610	4614	4618	4622	4626	4630	4634	4638	4642	4646	4650	4654	4658	4662	4666	4670	4674	4678	4682	4686	4690	4694	4698	4702	4706	4710	4714	4718	4722	4726	4730	4734	4738	4742	4746	4750	4754	4758	4762	4766	4770	4774	4778	4782	4786	4790	4794	4798	4802	4806	4810	4814	4818	4822	4826	4830	4834	4838	4842	4846	4850	4854	4858	4862	4866	4870	4874	4878	4882	4886	4890	4894	4898	4902	4906	4910	4914	4918	4922	4926	4930	4934	4938	4942	4946	4950	4954	4958	4962	4966	4970	4974	4978	4982	4986	4990	4994	4998	5002	5006	5010	5014	5018	5022	5026	5030	5034	5038	5042	5046	5050	5054	5058	5062	5066	5070	5074	5078	5082	5086	5090	5094	5098	5102	5106	5110	5114	5118	5122	5126	5130	5134	5138	5142	5146	5150	5154	5158	5162	5166	5170	5174	5178	5182	5186	5190	5194	5198	5202	5206	5210	5214	5218	5222	5226	5230	5234	5238	5242	5246	5250	5254	5258	5262	5266	5270	5274	5278	5282	5286	5290	5294	5298	5302	5306	5310	5314	5318	5322	5326	5330	5334	5338	5342	5346	5350	5354	5358	5362	5366	5370	5374	5378	5382	5386	5390	5394	5398	5402	5406	5410	5414	5418	5422	5426	5430	5434	54

2) Analyse des trames avec Wireshark

Le logiciel Wireshark est un analyseur de protocoles. Celui-ci peut utiliser directement l'interface de votre machine pour capturer des trames circulant sur le réseau.



- Lancez Wireshark et suivez l'enseignant pour la présentation de l'environnement

3) Etude détaillée de la commande ping avec Wireshark

Tache 1 :

- Lancez wireshark
- Lancez la capture sur l'interface Wireless dans la fenêtre Wireshark en spécifiant un filtre ICMP.
- Revenez au terminal sur votre machine et exécutez un **ping** vers le serveur dans votre salle TP en limitant le nombre de requêtes ICMP à 3.
- Retournez dans la fenêtre Wireshark et arrêtez la capture dès que la commande ping est terminée.
- Etudiez le résultat obtenu et renseignez les informations sur une trame ICMP.

Tache 2 :

La couche Ethernet

A partir de la capture réalisée précédemment complétez le tableau suivant:

+----- 48 bits -----+						+----- 48 bits -----+						+---16bits---+	
@MAC Source						@MAC Destination						Type	

Sachant que le champ **Type** peut avoir les valeurs: 0x0800 = IP
 0x0806 = ARP
 0x8035 = RARP

La couche IP

A partir de la capture réalisée précédemment complétez le tableau suivant:

+---4b---+		+---4b---+		+-----8b-----+				+--- 3b---+		+-----13b-----+			
Ver:	IHL:	TOS:		Longueur Totale:									
ID:				ind:	Fragment Offset:								
TTL:		Protocole:		Somme de ctrl d'entête:									
@IP source :													
@IP destination :													
.....													

Sachant que :

Ver = Version d'IP

IHL = Longueur de l'entête IP (en mots de 32 bits)

TOS = Ce champ permet de distinguer différentes qualité de service différenciant la manière dont les paquets sont traités. Composé de 3 bits de priorité (donc 8 niveaux) et trois indicateurs permettant de différencier le débit, le délai ou la fiabilité.

- Bits 0-2: Precedence.
- Bit 3: 0 = Normal Delay, 1 = Low Delay.
- Bits 4: 0 = Normal Throughput, 1 = High Throughput.
- Bits 5: 0 = Normal Reliability, 1 = High Reliability.
- Bit 6-7: Reserved for Future Use.

Longueur totale = Nombre total d'octets du datagramme, en-tête IP comprise.

ID (identificateur)= Numéro permettant d'identifier les fragments d'un même paquet.

Ind (indicateur) =

- Bit 1 : actuellement inutilisé.
- Bit 2 : DF (Don't Fragment) lorsque ce bit est positionné à 1, il indique que le paquet ne peut pas être fragmenté. Si le routeur

ne peut acheminer ce paquet (taille du paquet supérieure à la MTU), il est alors rejeté.

Bit 3 : MF (More Fragments) quand ce bit est positionné à 1, on sait que ce paquet est un fragment de données et que d'autres doivent suivre. Quand il est à 0, soit le fragment est le dernier, soit le paquet n'a pas été fragmenté.

Fragment Offset = Position du fragment par rapport au paquet de départ.

TTL = Time To Live. Ce champ indique le nombre maximal de routeurs à travers lesquels la trame peut passer. Ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit la trame. Cela évite l'encombrement du réseau.

Protocole = Ce champ indique quel protocole est utilisé

Quelques protocoles transportés :

- 1 = ICMP 8 = EGP
- 2 = IGMP 11 = GLOUP
- 4 = IP (encapsulation) 17 = UDP
- 5 = Stream 36 = XTP
- 6 = TCP 46 = RSVP

Somme de contrôle de l'en-tête ou Header Checksum = Ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de la trame.

Adresse IP source = Ce champ représente l'adresse IP de la machine émettrice.

Adresse IP destination = Adresse IP du destinataire du message.

Couche ICMP

A partir de la capture réalisée précédemment complétez le tableau suivant:

+-----8b-----+	+-----8b-----+	+-----16-----+
Type :	Code :	Somme ctrl :
.....		

Sachant que :

- Voici quelques types ICMP : 8 = Demande d'écho
- 0 = Réponse d'écho
- 11 = Durée de vie écoulée
- 12 Erreur de paramètre

3) Analyse des trames dans les réseaux sans fil

Ouvrir le fichier trace **Wireshark 802 11.pcap**. Cette trace a été collectée par AirPcap et wireshark dans un environnement plusieurs points d'accès. L'hôte collecteur est déjà associé à l'AP quand la trace commence.

En se basant sur le volet information au milieu de l'interface de WIRESHARK renseignez les informations suivantes :

- Quels sont les SSID des deux points d'accès émettant la plupart des trames **beacon** ?

.....

- Quel est l'intervalle de temps entre deux trames beacon dans chaque point d'accès.

.....

- Quel est la norme WiFi utilisé ?

.....

- Quel est le canal de transmission dans chaque PA ?

.....

- Les trames beacon du premier AP détecté avertissent qu'il supporte 4 débits de base et 8 Débits étendus. Quels sont ces débits ?

.....

- Dans la requête http quelle est l'adresse IP du domaine **gaia.cs.umass.edu**

.....
.....

- Observer les trames dans T 49 s, que s'est-il passer ?

.....
.....