

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and None. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server.

Security Mode :

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode :

Group Key Update Interval : (seconds)

PRE-SHARED KEY

Pre-Shared Key :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

تنظیمات مودم به پایان رسیده است. یک بار مودم را خاموش روشن کنید پس از حدود ۲ دقیقه چراغ Internet مودم به رنگ سبز روشن میشود که نشاندهنده اتصال صحیح به اینترنت است. در صورت وجود مشکل در اتصال به اینترنت مجدداً مراحل بالا را با دقت تکرار کنید.

۱.۳ آشنایی با سوئیچ

دستگاهی است که در قلب هر شبکه مبتنی بر روش استار قرار می گیرد. با استفاده از سوئیچ، چندین کاربر قادر به ارسال اطلاعات از طریق شبکه در یک لحظه خواهند بود. در سوئیچها سرعت ارسال اطلاعات هر یک از کاربران بر سرعت دستیابی سایر کاربران شبکه تاثیر نخواهد گذاشت. سوئیچها معمولاً در لایه ۲ مدل OSI هستند و با تعداد پورت ۵، ۸، ۱۶، ۲۴ و گاهی ۳۶ و ۴۸ پورت نیز تولید می شوند. سرعت آنها معمولاً 10/100 و یا ۱۰۰۰ مگابیت بر ثانیه است. سوئیچها دارای پورتهای RJ-45 و یا فیبر نوری و یا ترکیبی از هر دو هستند. در دو نوع رومیزی و رکمونت (نصب در رکهای ۱۹ اینچ استاندارد) وجود دارند.



برای کنترل و نگهداری شبکه های بزرگ و یا شبکه هایی که نیاز به پهنای باند زیاد و کنترل شده دارند نیاز به استفاده از سوئیچهای مدیریتی است. با اینگونه سوئیچها می توان تنظیمات متنوعی از قبیل پهنای باند، شبکه های مجازی، کنترل و گزارشات ترافیکی شبکه و ... را انجام داد. از مشخصاتی که تقریباً در تمام آنها مشترک است می توان به رکمونت بودن، تعداد ۲۴ پورت به بالا، امکان افزودن چندین نوع ماژول برای کاربردهای مختلف، وجود پورت سریال برای مدیریت مستقیم، امکان مدیریت از طریق وب، دارا بودن نرم افزار مدیریتی، پاورهای اضافی و قیمت بسیار بالا نسبت به سوئیچ های رایج اشاره کرد. سرعت سوئیچ کردن داخلی و همچنین حجم دیتای انتقالی در زمان واحد از جمله مشخصات مهم سوئیچها و تعیین کننده قیمت آنها می باشد. برخی از این سوئیچها امکان مدیریت در لایه ۲ شبکه و بالاتر را نیز دارند.



۱.۴ کامندهای کاربردی شبکه

دستورات مهمی که تو نت استفاده میشه با استفاده از اعلان فرمان:

Ping

با استفاده از این دستور می توان فعال بودن پروتکل TCP/IP و وضعیت ارتباطی کامپیوتر با کامپیوتر های دیگر و ادرس IP و نام میزبان را مشاهده کرد. بدین صورت که چهار بسته اطلاعاتی چهار بایت به سمت گیرنده ارسال می شود و در آن زمان رفت و برگشت نیز محاسبه می شود این دستور دارای پارمتر های زیر است:

-t با استفاده از این پارمتر ارسال و بسته ها بصورت متوالی تکرار می شود تا زمانیکه کار بران متوقف کند.

-a از این پارمتر برای یافتن نام میزبان از روی آدرس ip استفاده می شود.

Ipconfig

برای پیکر بندی پروتکل TCP/IP از آن استفاده می شود. در واقع همه اطلاعات کارت شبکه شامل نام میزبان ، نام سرویس دهنده اولیه و ثانویه DNS و آدرس IP الگو های زیر شبکه و آدرس دروازه اینترنت و آدرس کارت شبکه و نام درایو * را نشان می دهد و دارای پارمتر های زیر است:

ALL نام میزبان ، نام کارت شبکه و آدرس فیزیکی و به همراه وضعیت فعال یا غیر فعال بودن DHCP و آدرس DNS نمایش داده میشود.

Renew با اجرای این فرمان آی پی دریافت شده از DHCP تجدید شده و مجدداً آی پی جدید دریافت می شود.

release با اجرای این دستور آی پی پاک می شود.

Tracert

با استفاده از این دستور می توانیم مسیر ارتباطی بین کامپیوتر خود و یک آدرس IP خاص رو چک کنیم.

Netstat

به صورت پیش فرض اطلاعاتی که netstat به شما میدهد شامل انواع پروتکل هایی که در آن زمان استفاده می کنید ، local address ها و اطلاعات مربوط به پورتها یی که استفاده می کنند ، remote address ها و اطلاعات مربوط به پورتهایی که آنها نیز استفاده می کنند و در نهایت وضعیت جاری را نمایش می دهد. همانطور که پیداست این اطلاعات مشخص می کنند که چه ارتباطاتی برقرار و چه عملیاتی در حال انجام است و در زمان جاری کدام پورتهای سیستم باز و در حال تبادل اطلاعات و برقراری session هستند. در واقع ترافیک شبکه را کنترل می کند

nslookup

برای مشاهده رکوردهای DNS به صورت پیش فرض و یا سرور خاصی استفاده می شود.

فصل دوم

آشنایی با شبکه و انواع آن

۲.۱ کلاس های IP

IP Address (Internet Protocol Address)

ای پی (IP) یک آدرس منطقی که برای مشخص کردن دستگاه در ارتباط بین شبکه ها تعیین میشود از چهار رقم تشکیل شده است که با نقطه از هم جدا میشوند بطور مثال ۱۹۲.۱۶۸.۱۰.۲۰ هر عدد هشت بیت است که در مجموع میشود ۳۲ بیت $۴ * ۸ = ۳۲$ اعداد بکاربرده شده دسیمال هستند و بین ۰-۲۵۵ می باشند

همانطور که گفته شد هر ip address از ۳۲ bit تشکیل شده است و هر ip از چهار بخش تشکیل شده است که به هر بخش octet نیز گفته میشود بطور مثال ۱۹۲ یک octet میباشد

• IP Address Classes

متخصصان شبکه با توجه به نیاز شبکه تصمیم به استاندارد سازی و ایجاد کلاسهای مختلف شبکه نموده اند که با توجه به نیاز هر شبکه باید از آن استفاده نمود
ای پی آدرسها در ۵ کلاس رده بندی میشوند و عدد اول هر آدرس نشان دهنده کلاس آن آدرس است

Class A	1-126
Class B	128-191
Class C	192-223
Class D	224-239
Class E	240-254

مثلا ip ۱۰.۱۰.۱۰.۱ با توجه به اینکه رقم اول آن ۱۰ است نشان دهنده این اسنت که در کلاس **A** می باشد

ip ۱۹۲.۱۶۸.۱۰.۲۰ با توجه به اینکه رقم اول آن ۱۹۲ است نشان دهنده این است که در کلاس **C** می باشد

• Loop Back

اگر دقت کرده باشین عدد ۱۲۷ در کلاسهای فوق نبود به این دلیل است که این عدد برای چک کردن کارت شبکه مورد استفاده قرار میگیرد و اگر بخواهیم از صحت سالم بودن کارت شبکه اطمینان حاصل کنیم میتوانیم از این آدرس استفاده کنیم
ping 127.0.0.1

کلاس A

شبکه های کلاس A برای شبکه هایی که تعداد شبکه هایشان کم, ولیکن تعداد میزبانهایشان زیاد است و معمولا برای استفاده توسط انستیتوهای دولتی و آموزشی انتخاب میشوند مناسب هستند
در یک آدرس شبکه کلاس A, بخش نخست آن نشان دهنده آدرس شبکه (network address) و سه بخش دیگر نیز نشاندهنده آدرس میزبان (host address) در شبکه است. بطور مثال IP 10.20.20.20 عدد ۱۰ به آدرس شبکه و عدد ۲۰.۲۰.۲۰ به آدرس میزبان تعلق دارد
در آدرس دهی کلاس A اولین بیت صفر میباشد

$$01111111 = 0 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 127$$

کلاس B

شبکه های کلاس B برای شبکه هایی که تعداد شبکه هایشان بین شبکه های بسیار بزرگ و بسیار کوچک است در نظر گرفته شده است
در یک آدرس شبکه کلاس B دو بخش نخست آن نشان دهنده آدرس شبکه و دو بخش دیگر نشاندهنده آدرس میزبان است
بطور مثال IP 172.16.10.10 عدد ۱۷۲.۱۶ به آدرس شبکه تعلق دارد و عدد ۱۰.۱۰ به آدرس میزبان تعلق دارد
در آدرس دهی کلاس B دومین بیت صفر میباشد

$$10111111 = 128 + 0 + 32 + 16 + 8 + 4 + 2 + 1 = 191$$

کلاس C

شبکه های کلاس C برای شبکه هایی که تعداد شبکه های زیادی دارند اما میزبان کمتری دارند تدارک داده شده است
در یک آدرس شبکه کلاس C, سه بخش نخست آن نشان دهنده آدرس شبکه و بخش آخر به آدرس میزبان تعلق دارد
بطور مثال IP 192.168.10.20 عدد ۱۹۲.۱۶۸.۱۰ به آدرس شبکه و ۲۰ به آدرس میزبان تعلق دارد
در ای پی آدرس دهی کلاس C, سومین بیت صفر میباشد

$$11011111 = 128 + 64 + 0 + 16 + 8 + 4 + 2 + 1 = 223$$

کلاس D

آدرس کلاس D برای Multicasting استفاده میشود
بدلیل اینکه این آدرس رزرو شده است بهمین دلیل از بحث درباره آن خوداری میکنیم
در کلاس D چهارمین بیت صفر میباشد

$$11101111 = 128 + 64 + 32 + 0 + 8 + 4 + 2 + 1 = 239$$

Multicasting

فرایند ارسال یک پیام, همزمان به بیش از یک مقصد در شبکه را گویند

کلاس E

آدرسهای کلاس E برای research and Development استفاده میشود

در هر کلاس دو نوع IP Address (آدرس ای پی) موجود میباشد

آدرس ای پی خصوصی **Private address**
آدرس ای پی عمومی **public address**

Private address

برای تعیین شبکه های محلی استفاده میشود و برای استفاده از آنها احتیاج به هیچ مجوزی نیست

public address

برای تعیین شبکه های عمومی استفاده میشود و باید از سازمان **IANA** مجوز داشت

IANA(Internet Assigned Numbers Authority)

چگونه میتوان تشخیص داد ای پی عمومی است یا خصوصی ؟

برای IP های خصوصی یک رنج موجود میباشد اگر IP در آن رنج بود خصوصی است در غیر اینصورت IP عمومی است

Class	Private IP Address Range	Subnet Mask
A	10.0.0.0 to 10.255.255.255	255.0.0.0
B	172.16.0.0 to 172.31.255.255	255.240.0.0
C	192.168.0.0 to 192.168.255.255	255.255.0.0

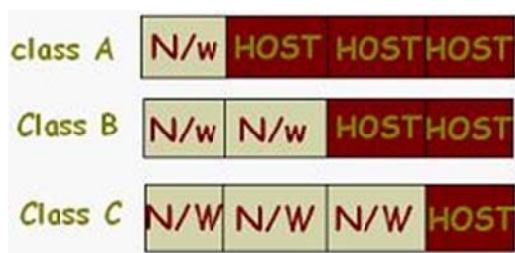
IDهای شبکه

فرض کنید شما در این آدرس سکونت دارید: اهواز کیانپارس خیابان ده پلاک ۶۰. اگر بخواهم یک نامه را از هند به شما بفرستم نمیتوانم فقط خیابان ده پلاک ۶۰ را بنویسم حتی اگر آن قسمت نمایانگر منزل شما باشد و اداره پست در ایران هم کمک نمیکند و برای اطمینان از صحت تحویل نامه آدرسهای پستی به ناحیه هایی تقسیم شده اند که کار را برای تحویل آن آسان میکند. آدرسهای IP نیز به این روش مشابه کار میکنند

هر IP از دو قسمت تشکیل شده است که قسمت اول متعلق به آدرس شبکه (**network address**) و قسمت دوم متعلق به آدرس میزبان (**host**) است

Network Address هر سیستم موجود بر روی شبکه مشابه ، به عنوان بخشی از آدرس IP آن در نظر گرفته میشود. بطور مثال IP 10.20.20.20 با توجه به اینکه IP از کلاس A میباشد عدد ۱۰ مشخص کننده آدرس شبکه در این IP است

Host Address هر سیستم موجود بر روی شبکه را مشخص میکند آدرس هاست بصورت منحصر بفرد میباشد زیرا این آدرس نشان دهنده یک سیستم خاص بر روی شبکه میباشد. بطور مثال IP 10.20.20.20 اعداد ۲۰.۲۰.۲۰ آدرس هاست را نشان میدهد



SUBNET MASK

این آدرس نشان میدهد چه مقدار بیت متعلق به آدرس شبکه و چه مقدار بیت متعلق به آدرس میزبان (هاست) است دو الگو برای subnet mask داریم الگوی استاندارد و الگوی غیر استاندارد در الگوی استاندارد با توجه به کلاس هر IP, subnet mask استاندارد برای آن ای پی داریم بطور مثال

Class	A	B	C
IP	10.10.10.1	172.168.88.98	192.168.100.3
Subnet Mask	255.0.0.0	255.255.0.0	255.255.255.0

قسمتی که ۲۵۵ است متعلق به network و قسمتی که ۰ است متعلق به host می باشد

بوسیله این فرمول میتوانیم تشخیص دهیم چه مقدار host و network در یک IP address موجود میباشد

$$2^n - 2$$

class	تعداد بیت‌های شبکه	تعداد بیت‌های میزبان	تعداد میزبان
A	8	24	$2^{24} - 2 = 16777214$
B	16	16	65534
C	24	8	254

الگوی غیراستاندارد

الگوهایی هستند که دقیقاً با محدودیتهای هشتایی مطابقت نمیکنند و در عوض برای نیازهای خاص طراحی شده اند، به این عملیات

subnetting میگویند

SUBNETTING

قرض دادن بیتهای هاست را به بیتهای شبکه subnetting میگویند

برای انجام دادن عملیات subnetting میبایست کار با عملیت باینری را بدانیم

اعداد باینری

اعداد باینری را برای نمایش آدرسها استفاده میکنند. اعداد باینری فرم اصلی نمایش اطلاعات روی یک ابزار کامپیوتر است. اعداد باینری فقط

شامل صفر و یک هستند که یک حالت ON و صفر حالت OFF در نظر گرفته میشود

سیستم باینری فقط یک روش متفاوت نمایش اعداد است

برای بدست آوردن عدد در مبنای باینری میبایست عدد را در مبنای دو تقسیم کرد و دوباره خارج قسمت را بر دو تقسیم کرد

عدد ۴ را میخواهیم به عدد باینری تبدیل کنیم

$$=0 \text{ باقیمانده } 4/2=2 \text{ --->}$$

$$=0 \text{ باقیمانده } 2/2=1 \text{ --->}$$

از بالا شروع میکنیم ۱۰۰

برای محاسبه از اولین باقیمانده شروع میکنم تا به آخری برسیم البته آخرین خارج قسمت را هم حساب میکنیم

تقسیم کردن اعداد بزرگ میتواند خسته کننده باشد بهمین جهت یک راه حل خیلی آسان و سریع ارائه میدهم

این اعداد را مدنظر داشته باشید

128 64 32 16 8 4 2 1

شما بفرض میخواهید عدد ۱۰ را به باینری تبدیل کنید. دقت کنید مجموع کدام از اعداد بالا ده میشود و جای آن اعداد یک و جای بقیه صفر

قرار میدهیم

$$10=2+8 \text{ -----> } 00001010$$

$$168=128+32+8 \text{ -----> } 10101000$$

$$192=128+64 \text{ -----> } 11000000$$

$$255=128+64+32+16+8+4+2+1 \text{ -----> } 11111111$$

