Network Protocols

Practical session 6

Sleman Khadoor
slemankhadoorit@gmail.com

Access Control List (ACL)

تستخدم قوائم التحكم بالوصول لإعطاء صلاحيات بالمنع أو السماح للمستخدمين بالوصول الى شبكات معينة، أو منع شبكات معينة من الوصول إلى شبكات أخرى، فمثلاً يمكن استخدامها لحماية شبكة داخلية من الشبكات الخارجية .كما يمكن تطبيق هذه الخدمة على بروتوكولات ومنافذ معينة كحجب موقع معين على البروتوكول HTTP، ومن ميزات ACLs أنها تمكننا من إعطاء الصلاحيات لجهاز حاسب خاص بمستخدم معين أوحجبها عنه دون التأثير على باقي الأجهزة المنتمية لنفس الشبكة وذلك بالاعتماد على عناوين هذه الأجهزة.

ويمكن القول أن قوائم التحكم بالوصول هي عبارة عن سلسلة من العبارات التي تعرف المعيار المستخدم للسماح أو لمنع نقل الرزم لواجهة معينة لموجه معين .حيث أن كل رزمة يتم اختبارها ومطابقتها مع العبارات الموجودة في قائمة الوصول من أجل محاولة الحصول على حالة تطابق مع أحد الشروط في القائمة.

استخدام قوائم الوصول يمكن أن نطلق عليه ما يسمى تنقية للرزم (Filtering)، ولكن يجب الإشارة إلى أن قوائم الوصول الموضوعة على موجه لايتم تفعيلها على الرزم التي يتم إنشاؤها من الموجه نفسه.

Wildcard mask

تستخدم قوائم الوصول ما يسمى بال wildcard mask لتحديد جهاز محدد أو مجال من الأجهزة الذي ستطبق عملية السماح أو المنع عليه ، الwildcard mask شكله مشابه لشكل ال subnet mask حيث يتكون من أربعة مقاطع، كل مقطع 8 bit ويتكون من أصفار تليها واحدات(من اليسار إلى اليمين).

تعني الأصفار أن البتات المقابلة لها في عنوان ال ip مهمة (هي التي تجري المقارنة على أساسها)، أما الواحدات فما يقابلها يمكن أن يتغير(غير مهم)، فمثلا عندما يكون عنوان ال ip بالشكل 192.168.1.1 وال wildcard mask بالشكل0.0.0.255

نكون قد ثبتنا أول 3 مقاطع والمقطع الأخير غير مهم مهما تغير، أي أن كل عنوان ip يماثل هذا العنوان في قيمة المقاطع الثلاث الأولى ستطبق عليه القائمة ولا تهم قيمة المقطع الأخير، ولكن عندما يكون ال wildcard mask بالشكل 0.0.0.0 نكون قد ثبتنا كامل العنوان وبالتالي ستطبق القائمة فقط على هذا العنوان.

يمثل الجدول في الصفحة التالية بعض الأمثلة التي ستساعدك على فهم الية استخدام ال wildcard mask في تحديد جهاز معين أو عدة أجهزة لتطبق عليها قائمة تحكم بالوصول.

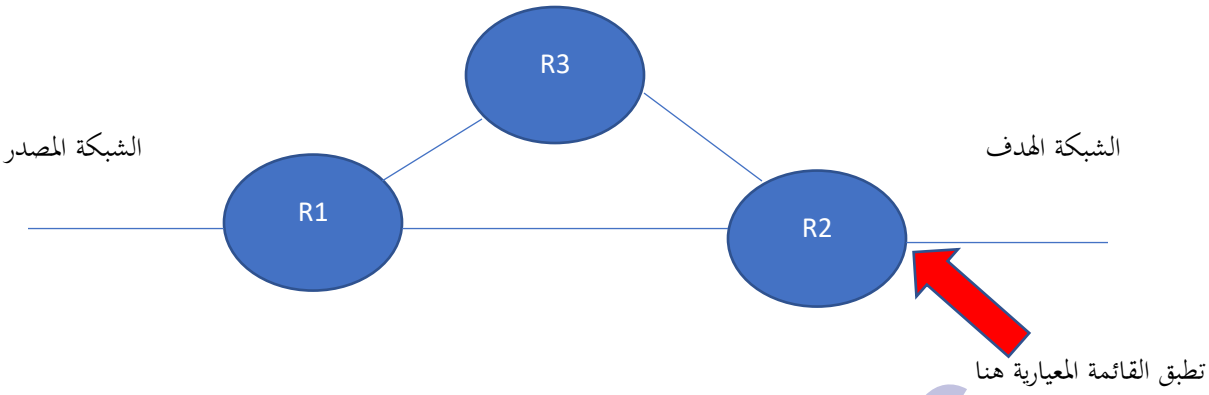
Address	Wildcard Mask	Match Result
0.0.0.0	255.255.255.255	جميع العناوين تحقق شروط قائمة الوصول
172.18.0.0	0.0.255.255	الشبكة 172.18.0.0
172.18.5.2	0.0.0.0	فقط الحاسب 172.18.5.2
172.18.8.0	0.0.0.7	فقط الشبكة الفرعية 172.18.8.0/29
172.18.8.8	0.0.0.7	فقط الشبكة الفرعية 172.18.8.8/29
172.18.8.15	0.0.0.3	فقط الشبكة الفرعية 172.18.8.12/30

أنواع قوائم التحكم بالوصول

- ✓ **قوائم الوصول المعيارية (Standard ACLs)**

تأخذ أرقام من 1 الى 99 وعادة نستخدم هذا النوع عندما نريد منع شبكة بالكامل من الوصول إلى شبكة أخرى دون تحديد حزم محددة، ويعتمد هذا النوع على عنوان المرسل فقط ويتم تطبيقها على الموجه (Router) الأقرب إلى الوجهة (Destination) التي نريد منع المرسل من الوصول اليها والمنفذ الأقرب الى الوجهة، وذلك لأن القائمة ستمنع عبور الرزم القادمة من الشبكة المصدر

نهائياً وبالتالي تطبق فقط على المنفذ المؤدي للشبكة الهدف، ويجب تحديد حالة المنفذ in أو out. وعادة في هذا النوع تكون حالة المنفذ out .



- ✓ **قوائم الوصول الموسعة (Extended ACLs)**

تأخذ أرقام من 100 الى 199 وعادة تستخدم عندما نريد تقييد الوصول لخدمات معينة مثل الانترنت، أو منع بروتوكول محدد من العمل ضمن الشبكة ومنع وصول بعض الحواسب الى أجزاء حساسة ضمن الشبكة مثل مخدم معين، وتعتمد على عنواني المرسل والوجهة معاً، ويتم تطبيق هذا النوع على الموجه (Router) الأقرب الى المرسل والمنفذ الأقرب الى المرسل الذي يكون بحالة (in). وذلك لأنه ما من داعٍ لعبور الرزم كامل الطريق ومن ثم إهمالها عند الوجهة، ومن شأن ذلك تقليل الازدحام، ولكن ليس من الخطأ تطبيقها على أي منفذ آخر ضمن الطريق.