Net Admin Weekly

59,000 Subscribers Worldwide

March 12 , 2003
Issue #28

CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters

CramSession

Feature

Q & A

Security Advisories

News Headlines & Resources

Download of the Week

Feature

to top

Fire and Water: Firewalls and Network Load Balancing, Multicast and Unicast

The Windows 2000 Network Load Balancing service (NLB) allows you to create an array or "cluster" of machines that all listen on the same IP address. When a host sends a packet to the NLB array address, all members of the NLB array receive the packet. This allows NLB to provide both fault tolerance and load balancing for communications destined for the array address.

NLB works great for servers that have all their interfaces on the same network segment. All packets destined for the array address end at the array address. The service may send responses from the array address back to the host that sent a request, but the responses go out through the same network on which the request was received.

Things aren't so simple when the server running NLB is a firewall. A firewall must have at least two network interfaces, and each interface must be on a different logical and physical segment. That's how firewalls do their work; they limit what packets can move between two separate and distinct networks. NLB can work great on a firewall, but there's just one problem: you can bind the NLB service to only one network interface per Windows 2000 computer. As you'll see in a little bit, this introduces a problem called "asymmetric routing". Let's take a high level overview of NLB before we get into issues NLB has with firewalls.

Unicast Mode

NLB can be configured to work in either unicast or multicast mode. These modes reflect the type of hardware address the NICs participating in the array use to listen for communications destined to the NLB array IP address.

NLB installs in unicast mode by default. In unicast mode, NLB replaces the actual MAC address of each adapter participating in the array with a unicast MAC address that is the same for all adapters participating in the NLB array. For example, if the array IP address is 10.0.0.1, an array unicast MAC address such as 02-bf-ac-10-00-01 replaces the individual MAC address on each adapter participating in the array.

The problem with unicast mode is that switches don't like to have the same MAC address registered on multiple ports. To get around this problem, NLB will "mask" the array MAC address with a bogus MAC address on each NIC participating in the array. This masking allows each NIC to register a different bogus MAC address on the switch port that its connected to while still allowing all array members to listen on the array MAC address.

How can each NIC register a different bogus MAC address on each switch port and still listen on a common NLB array MAC address? Switches (as opposed to routers with layer 2 awareness) are layer two devices. They are only aware of what's going on in the layer 2 Ethernet frame headers.

NLB puts the bogus MAC address in the Ethernet frame header; the switch analyzes the contents of the Ethernet header and that's how the switch learns the bogus MAC address.

Now you might be asking "how does the router get packets to all the array members if they're all listening on different MAC addresses?" That's a good question. If the router were only layer 2 aware it wouldn't be able to get packets to the NLB IP address because its needs to be layer 3 aware to even care about IP addresses.

It's this layer 3 awareness that allows NLB in unicast mode to present different MAC addresses to each switch port, but the same MAC address for the IP address used by all members of the array. Think about how the router learns the MAC address of a destination IP address. The router uses an ARP Request broadcast. What layer does ARP work on? The network layer – layer 3. When the upstream router issues an ARP Request broadcast for the IP address used by all members of the NLB array, the NLB service answers the ARP request with an ARP Reply containing the NLB MAC address in the ARP header. When you use NLB in unicast mode, the switch learns the bogus MAC address based on the layer 2 (Ethernet) header, and the upstream router learns the NLB array MAC address based on the layer 3 (ARP) header. Pretty smart!

The major limitation with unicast mode is that it introduces the problem of "switch flooding". When the router learns the NLB array MAC address, it sends the frames to that address. The switch receives these frames with the NLB array MAC address. The switch only knows about the bogus unicast MAC addresses it learned from the Ethernet frame headers; the switch has no record of the NLB array MAC address, so it sends the frames to all the ports in the switch.

Switch flooding is a problem if you have other servers connected to the same switch. The entire point of using a switch fabric instead of a shared hub is to allow each port in the switch full bandwidth. But if the router needs to send 10 Mbps of data to the NLB array MAC address, then the entire bandwidth available to all ports in the switch is used up by traffic destined to the array members because the switch can't partition the traffic to just the switch ports used by the array members (this example assumes this is 10 Mbps switch).

There is a way to get around this problem. Plug all the array members into a hub and then uplink the hub to the switch. Since none of the NLB array members are plugged into any of the switch ports, the switch is happy. In fact, you don't even need to mask the MAC addresses of the array members, because the hub doesn't care. However, we have a similar problem when using the hub: we can't take advantage of the full bandwidth available to all NLB array members. We're limited to the rated speed of the hub. This can be a major problem if we're trying to use Gigabit adapters to manage multiple connections or a multinet.

Multicast Mode

The other mode you can use with NLB is multicast modeMicrosoft probably would prefer multicast mode to be the default. However, there's a small problem with multicast mode and certain Cisco switches, so Microsoft has been good enough to defer to Cisco and make unicast mode the default. We'll get into the details of the problem in a little bit.

NLB multicast mode does not replace the IP address used by the adapters in the array. Each adapter keeps its original MAC address. NLB multicast mode doesn't need to change the MAC address on the NLB array adapters because all array members listen on a multicast MAC address. Switches allow multiple ports to listen on the same multicast MAC address, since that's the nature of multicasting.

NLB array members in multicast mode all listen on a multicast address like 03BFAC100001 (you can tell a multicast address from a unicast address because the low order digit of the high order octet is 1 for multicast and 0 for unicast). All adapters that listen on the address pass the frame up the stack and all adapters that don't listen on that multicast address drop the frame. The advantage of using multicast MAC addresses is that you can configure switches to forward frames to members of a multicast group. All other switch ports are unaffected by the traffic going to the NLB array members because you've programmed the switch to ignore multicast frames to ports that don't service NLB array members.

Sounds pretty good so far, but there's a problem (there's always a problem). Cisco interprets the RFCs differently than Microsoft, and so Cisco switches don't allow a unicast IP address to be associated with multicast MAC address. When the layer 3 "switch" does an ARP Request broadcast for the NLB array IP address, the NLB service will respond with a multicast MAC address. The Cisco device rejects this and no valid entry will exist in the Cisco devices ARP table.

This actually isn't a big deal. The technical solution is easy: just add a static entry in the router's ARP table. This entry has the NLB array IP address and the NLB Array MAC address. While the technical solution is easy, the psychosocial problems are less easy.

If you're a firewall administrator in a large corporation, there's a good chance that you manage the firewalls and network security infrastructure, and someone else manages the routers/switches. Because large organizations are inefficient, you'll probably have to ask someone else to make the static ARP table entry for you. Its likely that you'll get a lot of grief from this person, who's likely going to give you the "Cisco Good/Microsoft Bad" monologue. Who needs it? Because of these you're more likely to try and make unicast mode work.

Summary

The Windows 2000 NLB service allows multiple machines to listen on the same IP address on the same physical segment. This allows NLB to provide both load balancing and fault tolerance for the NLB array members. NLB can use either unicast mode or multicast mode to allow all the array members to receive all packets destined for the array. We discussed the advantages and disadvantages of each method. Next time we'll go over the problems you encounter when using NLB on multihomed firewalls.

This week's feature article by
Thomas W Shinder M.D., MCSE, etc.
Net Admin bi-Weekly Author
Co-Author, Configuring ISA Server 2000
Co-Author, ISA Server and Beyond

Q & A

Question: WINS Server Takes a Dump

Question:

Hi Dr. Tom,

I have problem joining my Windows 2000 Professional computer to my Windows 2000 Domain. I receive IP addressing information from a DHCP that is in segment #1 (192.168.1.x). The Domain Controller (DC1) for my domain (mycom) is located in segment #2 (192.168.2.x).I am able to ping DC1 and see the shared folders on that machine.

However, when I try to join the MYCOM domain, I receive an error message indicating that the client can't join the domain. My question: how can I join the domain when I'm currently located on a different segment? Please advise --Alan

Answer:

Hiya Alan! Looks like you might have a basic DNS issue here. First, I note you're using DHCP to assign IP addressing information to your network clients. Does the DHCP scope assign DNS server addresses to your clients? If so, make sure that DNS server knows about the domain you want the client to join. The DNS server should either have the appropriate SRV records, or a referral to a DNS server that is authoritative for the Active Directory domain. Something else to watch out for is the DNS settings on the client itself. You have the option to override the DHCP DNS settings at the client side, so check the TCP/IP Properties dialog box and make sure that someone has hard coded an incorrect DNS server address. Finally, the network ID isn't important – there appears to be a route between 192.168.1.0/24 and 192.168.2.0/24, so you don't need to worry about what subject the client is on unless the DHCP server doesn't have a scope for that network, and then you would know because the client wouldn't get a valid IP address and would not even be able to ping the Domain Controller.

Question: Is Outlook Web Access (OWA) Secure?

Question:

Dear Dr. Tom,

Has anybody ever used it? Looks like a pretty cool tool. I know it relies on IIS. Is it pretty secure? I have my Exchange server sitting behind a firewall in the inside network (not in the DMZ). I can lock it down pretty good with our Cisco PIX Firewall. I would just let http traffic to access it (and that is all). Any thoughts, or advice would be great! Thanks! --Chad

Answer:

Hey Chad, great question! You're right that OWA uses IIS to allow access to Exchange accounts using a Web interface. The level of security you have with OWA is the level of security you can provide for IIS. The first thing you should do is run the IISLockdown tool on the OWA Server. IISLockdown allows you to secure OWA and minimizes the chance of you DoS'ing yourself by setting the wrong security parameters. The next step after hardening the server is securing the link. While the PIX is OK for basic packet filtering, your OWA server security would be significantly improved if you used stateful, layer 7 aware firewall like ISA Server 2000. You can then use SSL to connect to the firewall and then to the OWA server on the internal network. You can significantly improve security by using client certificate authentication to authenticate with the ISA Server firewall, and then using basic authentication to authenticate with the OWA server. All credentials and data are secure due to SSL encryption. Good luck and enjoy OWA!

Security Advisories

Flaw in Windows Me Help and Support Center

to top

You can use the WinME Help and Support Center to get help and perform system diagnostics. Users and programs can execute URL links to Help and Support Center by using the "hcp://" prefix in a URL link instead of http://". A security vulnerability is present in the Windows Me version of Help and Support Center, and results because the URL Handler for the "hcp://" prefix contains an unchecked buffer. This is a critical security problem and you get the fix ASAP.

Read more...

Security Operations Guide for Windows 2000 Server

to top

How does Microsoft secure its own servers? You can be they use the principles and techniques outlined in their own Security Operations Guide for Windows 2000. You can download all 7 chapters and 7 appendices from this excellent online book.

Read more...

Inside Windows Update

to top

Here's an interesting expose on what information Windows Update collects and sends to Microsoft. They say that no "private" information is collected or sent, but if that's the case, why use SSL? The authors of this piece were able to tap into the WinInet API and get the info before it's encrypted.

Read more...

News Headlines and Resources

Bye, Bye, BIOS

to top

Alas, poor BIOS, I knew him well. The BIOS has been with us over decades, but now Intel says its going to be replaced with the new Extensible Firmware Interface (EFI). EFI promises to enhance ease of use and functionality for future computers, but beware: the dreaded DRM will benefit as well.

Read more...

The Insides of the Microsoft PPTP VPN Protocol

to top

There's a lot of noise about how secure IPSec is as a VPN protocol. But what about PPTP? Sure, PPTP has had its problems, but it's an extremely secure VPN protocol now, especially when you use EAP/TLS authentication.
This article provides you with juicy details on how PPTP communications work "under the hood".

Read more...

Network Access Quarantine Control

to top

One of the very cool new features in Windows 2003 is the new Network Access Quarantine Control facility. This new feature allows you to "quarantine" remote clients until a script can be run on the client machines to insure that they conform to network security policy. Check out this article for some of the details.

Read more...

Securing Data in Transit with IPSec

to top

You've locked down your Active Directory, users have complex passwords, and EFS is applied to all sensitive documents. The last step is to secure network communications with IPSec. In this article Deb Shinder shows you how it works and where to go for the next step.

Read more...

Windows 2003 Pricing Specs Released

to top

With the price of everything these days going through the roof, you'd think that Microsoft would increase the price of Windows 2003 over Windows 2000 to reflect increases due to inflation. Nope. Get Windows 2003 for the same price as Windows 2000, and if you want the Web version, its only $400US. Wow!

Read more...

Best Practice Active Directory Deployment for Managing Windows Networks

to top

Now that Windows NT 4.0 is on its last legs, are you thinking about rolling out a Windows 2000 Active Directory based network? First step is to read the Windows 2000 Resource Kit to learn the Active Directory basics. The next step is to check out Microsoft best practices. One word of warning, managing the Active Directory can be a nightmare, esp. in a large organization. Check out the second link for a cool piece of software that simplifies your Active Directory analysis and reporting.

Link one ...

Link two...

WebCast: W2K/2003 Server: Password & Account Lockout

to top

You will hear about security and administrative costs that you may see when you configure the password and account lockout feature set. This WebCast will provide information about configuring the password and account lockout settings, security and administrative considerations, new features in Microsoft Windows 2000 Server Service Pack 4 and Microsoft Windows Server 2003, procedures to troubleshoot account lockout events, and recommendations from the new account lockout white paper.

Read more...

Download of the Week

Irfanview

to top

It's a rare treat when you can find a freeware tool that does just about everything you want it to do. You'll find such a treat when you run IrfanView. Irfanview is the swiss army knife of graphics/media viewers. This puppy supports dozens of graphics formats, creates slideshows, performs batch conversions, extracts icons from DLL/EXE/ICL files, and doesn't require installation of any DLLs that might put you into DLL hell. While its FREEware, think about sending the programmer a couple of bucks if you like it.

Read more...