IPX-verkeer blokkeren met een EtherSwitch-filter op access point

Inhoud

Inleiding

Dit document legt uit hoe u EtherType-filters kunt gebruiken om IPX-verkeer (Internetwork Packet Exchange) op Cisco Aironet Access Point te blokkeren. Een typische situatie waarin dit nuttig is is wanneer de IPX server uitzendingen de draadloze verbinding verstikken, zoals soms op een groot ondernemingsnetwerk gebeurt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is van toepassing op Cisco Aironet access points die ofwel VxWorks ofwel Cisco IOS® software uitvoeren.

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de mogelijke impact van een opdracht begrijpt voordat u het gebruikt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Aansluiten op het access point

U kunt het beheersysteem van het access point openen via uw webbrowser of via de seriële poort van het access point met een terminalemulator. Als u niet bekend bent met de manier waarop u verbinding kunt maken met een access point, raadpleegt u De webbrowser-interface gebruiken voor aanwijzingen over hoe u verbinding kunt maken met een access point dat VxWorks draait of de Web-browser interface gebruiken om verbinding te maken met een access point dat Cisco IOS-software draait.

Configuratie

Access points die VxWorks uitvoeren

Nadat u een browser verbinding met het access point hebt gemaakt, voert u deze stappen uit om een filter te configureren en toe te passen om IPX-verkeer te blokkeren.

Een filter maken

Voer de volgende stappen uit:

1. Selecteer onder het menu Instellen de optie **EtherType-filters**.
2. Typ in het veld Naam instellen een filternaam (bijvoorbeeld "BlockIPX") en klik op **Add New**.
3. Op de volgende pagina ziet u de standaardlocatie. De twee opties zijn *vooruit* en *blokkeren*. Kies **vooruit** in het vervolgkeuzemenu.
4. Typ in het veld Speciale cases **0x8137** en klik op **Nieuw toevoegen**.
5. Er verschijnt een nieuw venster met deze opties:ontbindingPrioriteitOngekende tijd-tot-levenMulticast voor tijd-tot-bewegende apparatenwaarschuwenKies voor de ontbinding **Blokken**. Laat de andere opties bij hun standaardinstellingen. Klik op **OK**.U wordt teruggestuurd naar het EtherSwitch-scherm. Herhaal Stap 4 en Stap 5, en voeg types **0x8138**, **0x00ff** en **0x00e0 toe**.

Het filter toepassen

Als het filter eenmaal is gemaakt, moet deze op de interface worden toegepast om effect te sorteren.

1. Naar de setup-pagina terugkeren. Klik onder het gedeelte Netwerkpoorten op de rij met gemarkeerd Ethernet op **Filters**.
2. U ziet EtherType met Ontvang en Vooruit instellingen. Kies in elk uitrolmenu het filter dat u in Stap 2 van de procedure Filter hebt gemaakt en klik op **OK**. Met deze stap wordt het filter dat u hebt gemaakt, geactiveerd.

Access points voor Cisco IOS-software

Een filter maken

Voer de volgende stappen uit:

1. Klik op **Services** in de pagina-navigatiebalk.
2. Klik in de lijst Servicespagina op **Filters**.
3. Klik in de pagina Filters toepassen op het tabblad **EtherType Filters** boven op de pagina.
4. Zorg ervoor dat **NIEUW** (de standaard) is geselecteerd in het menu Filterindex maken/bewerken. Als u een bestaand filter wilt bewerken, selecteert u het filternummer in het menu Filterindex maken/bewerken.
5. In het veld Filter index noemt u het filter met een nummer van 200 tot 299. Het nummer dat u toevoegt, maakt een toegangscontrolelijst (ACL) voor het filter.
6. Voer **0x8137** in het veld EtherType toevoegen.
7. Laat het masker voor EtherSwitch in het veld masker bij de standaardwaarde.
8. Kies **Blok** in het menu Actie.
9. Klik op **Add** (Toevoegen). EtherType verschijnt in het veld Filters Classes.
10. Als u EtherSwitch uit de lijst Filters wilt verwijderen, selecteert u deze en vervolgens klikt u op **Klasse verwijderen**. Herhaal Stap 6 tot en met Stap 9 en voeg **de** typen **0x8138**, **0x00ff** en **0x00e0** aan het filter toe.
11. Klik op **Voorwaarts Alle** opties in het menu Standaardactie. Omdat u alle IPX-pakketten met dit filter blokkeert, moet u een standaardactie hebben die op alle andere pakketten van toepassing is.
12. Klik op **Apply** (Toepassen).

Het filter toepassen

Het filter is op dit punt opgeslagen op het access point, maar het is niet ingeschakeld totdat u het op de pagina Filters toepassen toepast.

1. Klik op het tabblad **Filters toepassen** om terug te keren naar de pagina Filters toepassen.
2. Selecteer het filternummer in een van de vervolgkeuzemenu EtherType. U kunt het filter op of zowel de Ethernet- als radiopoorten en op of zowel inkomende en uitgaande pakketten toepassen.
3. Klik op **Apply** (Toepassen). Het filter is op de geselecteerde poorten ingeschakeld.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Productondersteuning voor draadloos LAN

- Ondersteuning voor draadloze LAN-technologie
- Draadloze LAN-software
- Technische ondersteuning en documentatie – Cisco Systems