(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-88747
(P2004-88747A)
(43)公開日　平成16年3月18日(2004.3.18)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/28	H04L	12/28　200A	5K033

審査請求 未請求　請求項の数 31　ＯＬ　（全 32 頁）

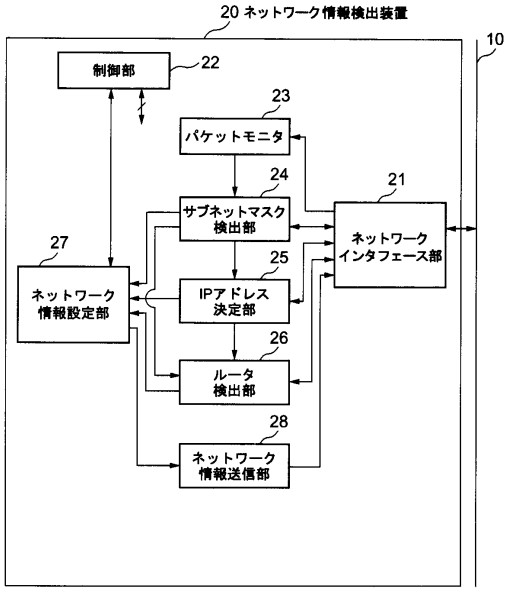
(21)出願番号　特願2003-180537(P2003-180537)
(22)出願日　平成15年6月25日(2003.6.25)
(31)優先権主張番号　特願2002-191717(P2002-191717)
(32)優先日　平成14年7月1日(2002.7.1)
(33)優先権主張国　日本国(JP)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100097157
弁理士　桂木　雄二
(72)発明者　嶋田　昌生
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5K033 CB13　CC01　EA06　EC03

(54)【発明の名称】ネットワーク情報検出装置および方法

(57)【要約】
【課題】ネットワーク情報を提供するサーバ機能を必要とせずに、ネットワーク情報の検出を実現できるネットワーク情報検出装置を提供する。
【解決手段】複数の機器が接続されたＬＡＮ上のパケットをモニタするパケットモニタ（２３）と、モニタされた少なくとも１個のパケットに含まれるＩＰアドレスに基づいて当該ＩＰアドレスを使用するネットワーク機器に設定されたサブネットマスクを検出するサブネットマスク検出部（２４）と、を有する。モニタされたパケットに含まれる送信先ＩＰアドレスと送信先ＭＡＣアドレスとが同一のネットワーク機器を指示しない場合、当該送信先ＭＡＣアドレスに対応するＩＰアドレスをルータのＩＰアドレスとして検出するルータ検出部（２６）を有する。
【選択図】　図２



【特許請求の範囲】
【請求項１】
複数のネットワーク機器が接続されたローカルネットワークのネットワーク情報を検出する装置において、
前記ローカルネットワーク上のパケットをモニタするパケットモニタ手段と、
前記パケットモニタ手段によりモニタされた少なくとも１個のパケットに含まれるＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスに基づいて、前記モニタされたパケットに関係するネットワーク機器に設定されたサブネットマスクを検出するサブネットマスク検出手段と、
を有することを特徴とするネットワーク情報検出装置。
【請求項２】
前記サブネットマスク検出手段は、前記モニタされた少なくとも１個のパケットに含まれる送信元ＩＰアドレスおよび送信先ＩＰアドレスの最大ＩＰアドレスと最小ＩＰアドレスとを求め、前記最大ＩＰアドレスおよび前記最小ＩＰアドレスのサブネットホスト部における異なるビットの最上位を特定することで前記サブネットマスクを検出することを特徴とする請求項１記載のネットワーク情報検出装置。
【請求項３】
前記サブネットマスク検出手段は、モニタされた複数のパケットの各々に含まれる送信元ＩＰアドレスおよび送信先ＩＰアドレスから各パケットのＩＰ領域を求め、前記モニタされた複数のパケットのＩＰ領域が重なる場合にはそれらを１つのＩＰ領域とし、最終的に求められた少なくとも１個のＩＰ領域から最大ＩＰアドレスと最小ＩＰアドレスとを求め、前記最大ＩＰアドレスおよび前記最小ＩＰアドレスのサブネットホスト部における異なるビットの最上位を特定することで前記サブネットマスクを検出することを特徴とする請求項１記載のネットワーク情報検出装置。
【請求項４】
前記サブネットマスク検出手段は、モニタされた１個のパケットに含まれるＩＰアドレスとネットワーク層で通信可能な他のＩＰアドレスの範囲を求め、当該ＩＰアドレス範囲に従って前記サブネットマスクを検出することを特徴とする請求項１記載のネットワーク情報検出装置。
【請求項５】
さらに、
前記サブネットマスク検出手段により検出されたサブネットマスクにより示されるサブネット内のＩＰアドレスに対してＡＲＰ要求を送信し、ＡＲＰ応答が返信されないＩＰアドレスを割当可能なＩＰアドレスとして決定するＩＰアドレス決定手段
を有することを特徴とする請求項１記載のネットワーク情報検出装置。
【請求項６】
さらに、
前記サブネットマスク検出手段により検出されたサブネットマスクにより示されるサブネット内のＩＰアドレスに対してＩＣＭＰエコー要求を順次送信し、それに対するＩＣＭＰ応答からルータのＩＰアドレスを検出するルータ検出手段
を有することを特徴とする請求項１記載のネットワーク情報検出装置。
【請求項７】
前記ＩＣＭＰ応答はＩＣＭＰ経路変更要求メッセージおよびＩＣＭＰ時間切れメッセージのいずれかであることを特徴とする請求項６記載のネットワーク情報検出装置。
【請求項８】
さらに、
前記パケットモニタ手段によりモニタされたパケットに含まれる送信先ＩＰアドレスと送信先ＭＡＣアドレスとが同一のネットワーク機器を指示しない場合、当該送信先ＭＡＣアドレスに対応するＩＰアドレスをルータのＩＰアドレスとして検出するルータ検出手段
を有することを特徴とする請求項１記載のネットワーク情報検出装置。

【請求項９】
さらに、
ＩＣＭＰのエコー要求およびエコー応答機能を用いて、モニタされたＩＰアドレスを使用している他のネットワーク機器のサブネットマスクと自己のサブネットマスクとの同一性を判定するサブネットマスク同一性判定手段
を有し、前記他のネットワーク機器のサブネットマスクと前記自己のサブネットマスクとが異なる場合、前記サブネットマスク検出手段により当該他のネットワーク機器のサブネットマスクを検出することを特徴とする請求項１記載のネットワーク情報検出装置。
【請求項１０】
複数のネットワーク機器が接続されたローカルネットワークのネットワーク情報を検出する装置において、
前記ローカルネットワーク上のパケットをモニタするパケットモニタ手段と、
前記パケットモニタ手段によりモニタされたパケットに含まれる送信先ＩＰアドレスと送信先ＭＡＣアドレスとが同一のネットワーク機器を指示しない場合、当該送信先ＭＡＣアドレスに対応するＩＰアドレスをルータのＩＰアドレスとして検出するルータ検出手段と、
を有することを特徴とするネットワーク情報検出装置。
【請求項１１】
複数のネットワーク機器が接続されたローカルネットワークにおけるネットワーク情報を検出する方法において、
ａ）前記ローカルネットワーク上のパケットをモニタするステップと、
ｂ）モニタされた少なくとも１個のパケットに含まれるＩＰアドレスに基づいて、前記モニタされたパケットに関係するネットワーク機器に設定されたサブネットマスクを検出するステップと、
を有することを特徴とするネットワーク情報検出方法。
【請求項１２】
前記ステップｂ）は、
前記モニタされた少なくとも１個のパケットに含まれる送信元ＩＰアドレスおよび送信先ＩＰアドレスの最大ＩＰアドレスと最小ＩＰアドレスとを検出し、
前記最大ＩＰアドレスおよび前記最小ＩＰアドレスのサブネットホスト部における異なるビットのうち最上位を特定し、
前記異なる最上位ビットより１つ上位のビットから上位すべてのビットをセット状態とし、前記異なる最上位ビット以下のビットをすべてリセット状態にすることで前記サブネットマスクを生成する、
ことを特徴とする請求項１１記載のネットワーク情報検出方法。
【請求項１３】
前記ステップｂ）は、
モニタされた複数のパケットの各々に含まれる送信元ＩＰアドレスおよび送信先ＩＰアドレスから各パケットのＩＰ領域を生成し、
前記モニタされた複数のパケットのＩＰ領域が互いに重なる場合にはそれらを１つのＩＰ領域に結合し、
最終的に求められた少なくとも１個のＩＰ領域から最大ＩＰアドレスと最小ＩＰアドレスとを検出し、
前記最大ＩＰアドレスおよび前記最小ＩＰアドレスのサブネットホスト部における異なるビットのうち最上位を特定し、
前記異なる最上位ビットより１つ上位のビットから上位すべてのビットをセット状態とし、前記異なる最上位ビット以下のビットをすべてリセット状態にすることで前記サブネットマスクを生成する、
ことを特徴とする請求項１１記載のネットワーク情報検出方法。
【請求項１４】

前記ステップｂ）は、
モニタされた１個のパケットからモニタＩＰアドレスを検出し、
前記モニタＩＰアドレスから増加する方向および減少する方向へ１ビットずつ変化させた検査ＩＰアドレスを順次生成し、
生成された検査ＩＰアドレスと前記モニタＩＰアドレスとの間でネットワーク層での通信が可能か否かを判定し、
前記増加する方向および減少する方向のそれぞれの方向においてネットワーク層での通信が初めてできなくなった時のビット位置のうち上位のビットを特定し、
前記上位ビットより１つ上位のビットから上位すべてのビットをセット状態にし、前記上位ビット以下のビットをすべてリセット状態にすることで前記サブネットマスクを生成する、
ことを特徴とする請求項１１記載のネットワーク情報検出方法。
【請求項１５】
さらに、
ｃ）検出されたサブネットマスクにより示されるサブネット内のＩＰアドレスに対してＡＲＰ要求を送信し、
ｄ）ＡＲＰ応答が返信されないＩＰアドレスを割当可能なＩＰアドレスとして決定する
を有することを特徴とする請求項１１記載のネットワーク情報検出方法。
【請求項１６】
さらに、
ｃ）モニタされたパケットに含まれる送信先ＩＰアドレスと送信先ＭＡＣアドレスとが同一のネットワーク機器を指示しない場合、当該送信先ＭＡＣアドレスをターゲットハードウエアアドレスとするＩｎＡＲＰ要求を送信し、
ｄ）前記ＩｎＡＲＰ要求に対するＩｎＡＲＰ応答を受信した場合に、前記ＩｎＡＲＰ応答に含まれる送信元ＩＰアドレスをルータのＩＰアドレスとして検出する
ことを特徴とする請求項１１記載のネットワーク情報検出方法。
【請求項１７】
さらに、
ｃ）検出されたサブネットマスクにより示されるサブネット内のＩＰアドレスを検査ＩＰアドレスとして順次生成し、検査ＩＰアドレスに対してＩＣＭＰエコー要求を送信し、
ｄ）前記ＩＣＭＰエコー要求に対してＩＣＭＰ経路変更要求を受信すれば、当該ＩＣＭＰ経路変更要求からルータのＩＰアドレスを検出し、
ｅ）前記ＩＣＭＰエコー要求に対してＩＣＭＰ時間切れを受信すれば、当該ＩＣＭＰ時間切れの送信元ＩＰアドレスをルータのＩＰアドレスとして検出する、
ことを特徴とする請求項１１記載のネットワーク情報検出方法。
【請求項１８】
さらに、
ｃ）ＩＣＭＰのエコー要求およびエコー応答機能を用いて、モニタされたＩＰアドレスを使用している他のネットワーク機器のサブネットマスクと自己のサブネットマスクとの同一性を判定し、
ｄ）前記他のネットワーク機器のサブネットマスクと前記自己のサブネットマスクとが異なる場合、前記ステップｂ）を実行する、
ことを特徴とする請求項１１記載のネットワーク情報検出方法。
【請求項１９】
複数のネットワーク機器が接続されたローカルネットワークにおけるネットワーク情報を検出する方法において、
ａ）前記ローカルネットワーク上のパケットをモニタするステップと、
ｂ）モニタされたパケットに含まれる送信先ＩＰアドレスと送信先ＭＡＣアドレスとが同一のネットワーク機器を指示しない場合、当該送信先ＭＡＣアドレスをターゲットハードウエアアドレスとするＩｎＡＲＰ要求を送信するステップと、

ｃ）前記ＩｎＡＲＰ要求に対するＩｎＡＲＰ応答を受信した場合に、前記ＩｎＡＲＰ応答に含まれる送信元ＩＰアドレスをルータのＩＰアドレスとして検出するステップと、
を有することを特徴とするネットワーク情報検出方法。
【請求項２０】
複数のネットワーク機器が接続されたローカルネットワークにおけるネットワーク情報を検出する方法において、
ａ）前記ローカルネットワーク上のパケットをモニタするステップと、
ｂ）モニタされたパケットのＩＰアドレス（以下、モニタＩＰアドレスという。）のネットワークアドレスと自己のネットワークアドレスとを比較するステップと、
ｃ）ネットワークアドレスが同一の場合、ＩＣＭＰのエコー要求およびエコー応答機能を用いて、前記モニタＩＰアドレスを使用している他のネットワーク機器のサブネットマスクと自己のサブネットマスクとの同一性を判定するステップと、
を有することを特徴とするネットワーク情報検出方法。
【請求項２１】
前記ステップｃ）は、
ｃ．１）前記自己のＩＰアドレスおよび前記モニタＩＰアドレスのいずれかのホスト部をすべて０およびすべて１のいずれかに設定した送信元ＩＰアドレスを有するＩＣＭＰエコー要求を前記他のネットワーク機器へ送信し、
ｃ．２）前記他のネットワーク機器から前記ＩＣＭＰエコー要求に対するＩＣＭＰエコー応答をユニキャストで受信した場合、自己のサブネットマスク値は前記他のネットワーク機器のそれより大きいと判定し、
ｃ．３）前記他のネットワーク機器から前記ＩＣＭＰエコー応答がない場合およびブロードキャストで受信した場合のいずれかの場合には、自己のサブネットマスク値は前記他のネットワーク機器のそれ以下であると判定する、
ことを特徴とする請求項２０記載のネットワーク情報検出方法。
【請求項２２】
さらに、
ｃ．４）前記ステップｃ．３）において、自己のサブネットマスク値は前記他のネットワーク機器のそれ以下であると判定された場合、前記自己のＩＰアドレスおよび前記モニタＩＰアドレスのいずれかのホスト部の少なくとも最上位ビットを反転させた送信元ＩＰアドレスを有するＩＣＭＰエコー要求を前記他のネットワーク機器へ送信し、
ｃ．５）前記他のネットワーク機器から前記ＩＣＭＰエコー要求に対するＩＣＭＰエコー応答をユニキャストで受信した場合、自己のサブネットマスク値は前記他のネットワーク機器のそれより小さいと判定し、
ｃ．６）前記他のネットワーク機器から前記ＩＣＭＰエコー応答がない場合には、自己のサブネットマスク値と前記他のネットワーク機器のそれとは等しいと判定する、
ことを特徴とする請求項２１記載のネットワーク情報検出方法。
【請求項２３】
前記ステップｃ）は、
ｃ．１）　前記自己のＩＰアドレスおよび前記モニタＩＰアドレスのいずれかのホスト部の少なくとも最上位ビットを反転させた送信元ＩＰアドレスを有するＩＣＭＰエコー要求を前記他のネットワーク機器へ送信し、
ｃ．２）前記他のネットワーク機器から前記ＩＣＭＰエコー要求に対するＩＣＭＰエコー応答をユニキャストで受信した場合、自己のサブネットマスク値は前記他のネットワーク機器のそれ以上であると判定し、
ｃ．３）前記他のネットワーク機器から前記ＩＣＭＰエコー応答がない場合には、自己のサブネットマスク値は前記他のネットワーク機器のそれより小さいと判定する、
ことを特徴とする請求項２０記載のネットワーク情報検出方法。
【請求項２４】
さらに、

ｃ．４）前記ステップｃ．２）において、自己のサブネットマスク値は前記他のネットワーク機器のそれ以上であると判定された場合、前記自己のＩＰアドレスおよび前記モニタＩＰアドレスのいずれかのホスト部をすべて０およびすべて１のいずれかに設定した送信元ＩＰアドレスを有するＩＣＭＰエコー要求を前記他のネットワーク機器へ送信し、
ｃ．５）前記他のネットワーク機器から前記ＩＣＭＰエコー要求に対するＩＣＭＰエコー応答をユニキャストで受信した場合、自己のサブネットマスク値は前記他のネットワーク機器のそれより大きいと判定し、
ｃ．６）前記他のネットワーク機器から前記ＩＣＭＰエコー応答がない場合およびブロードキャストで受信した場合のいずれかの場合には、自己のサブネットマスク値と前記他のネットワーク機器のそれとは等しいと判定する、
ことを特徴とする請求項２３記載のネットワーク情報検出方法。

【請求項２５】

さらに、
ｃ．４）前記ステップｃ．２）において、自己のサブネットマスク値は前記他のネットワーク機器のそれ以上であると判定された場合、前記自己のＩＰアドレスおよび前記モニタＩＰアドレスのいずれかのネットワークアドレスの最下位ビットを反転させた送信元ＩＰアドレスを有するＩＣＭＰエコー要求を前記他のネットワーク機器へ送信し、
ｃ．５）前記他のネットワーク機器から前記ＩＣＭＰエコー要求に対するＩＣＭＰエコー応答をユニキャストで受信した場合、自己のサブネットマスク値は前記他のネットワーク機器のそれより大きいと判定し、
ｃ．６）前記他のネットワーク機器から前記ＩＣＭＰエコー応答がない場合には、自己のサブネットマスク値と前記他のネットワーク機器のそれとは等しいと判定する、
ことを特徴とする請求項２３記載のネットワーク情報検出方法。

【請求項２６】

前記ステップｃ）は、
ｃ．１）　前記自己のＩＰアドレスおよび前記モニタＩＰアドレスのいずれかのネットワークアドレスの最下位ビットを反転させた送信元ＩＰアドレスを有するＩＣＭＰエコー要求を前記他のネットワーク機器へ送信し、
ｃ．２）前記他のネットワーク機器から前記ＩＣＭＰエコー要求に対するＩＣＭＰエコー応答をユニキャストで受信した場合、自己のサブネットマスク値は前記他のネットワーク機器のそれより大きいと判定し、
ｃ．３）前記他のネットワーク機器から前記ＩＣＭＰエコー応答がない場合には、自己のサブネットマスク値は前記他のネットワーク機器のそれ以下であると判定する、
ことを特徴とする請求項２０記載のネットワーク情報検出方法。

【請求項２７】

さらに、
ｃ．４）前記ステップｃ．３）において、自己のサブネットマスク値は前記他のネットワーク機器のそれ以下であると判定された場合、前記自己のＩＰアドレスおよび前記モニタＩＰアドレスのいずれかのホスト部の少なくとも最上位ビットを反転させた送信元ＩＰアドレスを有するＩＣＭＰエコー要求を前記他のネットワーク機器へ送信し、
ｃ．５）前記他のネットワーク機器から前記ＩＣＭＰエコー要求に対するＩＣＭＰエコー応答をユニキャストで受信した場合、自己のサブネットマスク値は前記他のネットワーク機器のそれと等しいと判定し、
ｃ．６）前記他のネットワーク機器から前記ＩＣＭＰエコー応答がない場合には、自己のサブネットマスク値は前記他のネットワーク機器のそれより小さいと判定する、
ことを特徴とする請求項２６記載のネットワーク情報検出方法。

【請求項２８】

複数のネットワーク機器が接続されたローカルネットワークにおけるネットワーク情報を検出する方法において、
ａ）前記ローカルネットワーク上のＡＲＰパケットをモニタするステップと、

ｂ）モニタされたＡＲＰパケットのＩＰアドレス（以下、モニタＩＰアドレスという。）のネットワークアドレスと自己のネットワークアドレスとを比較するステップと、
ｃ）ネットワークアドレスが同一の場合、ＩＣＭＰエコー要求を前記モニタＩＰアドレスを使用している他のネットワーク機器へ送信し、
ｄ）前記ＩＣＭＰエコー要求に対するＩＣＭＰエコー応答の有無に応じて、前記他のネットワーク機器のサブネットマスク値と自己のサブネットマスク値との同一性を判定するステップと、
を有することを特徴とするネットワーク情報検出方法。
【請求項２９】
コンピュータに、複数のネットワーク機器が接続されたローカルネットワークにおけるネットワーク情報を検出するように動作させるネットワーク情報検出プログラムにおいて、
ａ）前記ローカルネットワーク上のパケットをモニタするステップと、
ｂ）モニタされた少なくとも１個のパケットに含まれるＩＰアドレスに基づいて、前記モニタされたパケットに関係するネットワーク機器に設定されたサブネットマスクを検出するステップと、
を有することを特徴とするネットワーク情報検出プログラム。
【請求項３０】
コンピュータに、複数のネットワーク機器が接続されたローカルネットワークにおけるネットワーク情報を検出するように動作させるネットワーク情報検出プログラムにおいて、
ａ）前記ローカルネットワーク上のパケットをモニタするステップと、
ｂ）モニタされたパケットに含まれる送信先ＩＰアドレスと送信先ＭＡＣアドレスとが同一のネットワーク機器を指示しない場合、当該送信先ＭＡＣアドレスをターゲットハードウエアアドレスとするＩｎＡＲＰ要求を送信するステップと、
ｃ）前記ＩｎＡＲＰ要求に対するＩｎＡＲＰ応答を受信した場合に、前記ＩｎＡＲＰ応答に含まれる送信元ＩＰアドレスをルータのＩＰアドレスとして検出するステップと、
を有することを特徴とするネットワーク情報検出プログラム。
【請求項３１】
コンピュータに、複数のネットワーク機器が接続されたローカルネットワークにおけるネットワーク情報を検出するように動作させるネットワーク情報検出プログラムにおいて、
ａ）前記ローカルネットワーク上のパケットをモニタするステップと、
ｂ）モニタされたパケットのＩＰアドレス（以下、モニタＩＰアドレスという。）のネットワークアドレスと自己のネットワークアドレスとを比較するステップと、
ｃ）ネットワークアドレスが同一の場合、ＩＣＭＰのエコー要求およびエコー応答機能を用いて、前記モニタＩＰアドレスを使用している他のネットワーク機器のサブネットマスクと自己のサブネットマスクとの同一性を判定するステップと、
を有することを特徴とするネットワーク情報検出プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はネットワークシステムにおけるネットワーク情報の自動取得技術に係り、特にサブネットマスクやルータＩＰアドレスなどのネットワーク情報を検出する装置および方法に関する。
【０００２】
【従来の技術】
コンピュータをネットワークに接続するには、サブネットマスク、ＩＰアドレス、ルータアドレス等のネットワーク情報を取得してコンピュータに設定する必要がある。このようなネットワーク情報は手動で設定することもできるが、人手による設定にはネットワークの知識を必要とし、ネットワーク情報を調査する手間もかかる。また、誤ってネットワーク情報を設定した場合はネットワーク全体を混乱させることもありうる。
【０００３】

他方、ＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）サーバが存在する場合には、ネットワーク情報をＤＨＣＰサーバから自動的に取得することができる。しかしながら、ネットワーク情報の自動取得を行うには、ネットワーク情報の提供を目的としたサーバを構築しなければならない。

【０００４】

特開２００２－１９０８１１号公報（特許文献１）には、ネットワーク上の装置のＩＰアドレスやサブネットマスクなどを自動的に取得する方法が開示されている。この従来の方法では、ネットワーク情報をＤＨＣＰサーバから取得できない場合に、ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）アドレスマスク要求を送信し、その応答およびネットワーク・トラフィックから有効なサブネットを決定する（段落番号００１８～００２１）。そして、決定されたサブネット内で、未使用ＩＰアドレスの検出やＩＣＭＰルータ選択メッセージを用いたデフォルトルータの検出を実行する（段落番号００２５～００２７）。

【０００５】

【特許文献１】

特開２００２－１９０８１１号公報（段落番号００２５～００２７、要約、図３～５）。

【０００６】

【発明が解決しようとする課題】

しかしながら、特許文献１に開示されたＩＰ構成自動取得方法では、ＩＣＭＰアドレスマスク要求をネットワークに送信し、それに対する応答を用いてサブネットマスクを検出しているために、ネットワークの負荷が増大するだけでなくサブネットマスク検出を高速化することができない。また、従来のルータ検出方法では、ＲＦＣ１２５６に記述されているルータのＩＰアドレス検出方法をそのまま用いているだけであり、ルータ検出の高速化については考慮されていない。また、ＩＣＭＰルータ選択メッセージをサポートしていないルータが存在するために、従来の方法ではルータを検出できない場合がある。

【０００７】

本発明の目的は、ネットワーク情報を提供するサーバ機能を必要とせずに、ネットワーク情報を自動かつ高速で取得することができるネットワーク情報検出装置及び方法を提供することにある。

【０００８】

本発明の他の目的は、サブネットマスクを高速検出可能なネットワーク情報検出装置及び方法を提供することにある。

【０００９】

本発明のさらに他の目的は、ルータＩＰアドレスを高速検出可能なネットワーク情報検出装置及び方法を提供することにある。

【００１０】

【課題を解決するための手段】

本発明によれば、複数のネットワーク機器が接続されたローカルネットワークのネットワーク情報を検出する装置において、前記ローカルネットワーク上のパケットをモニタするパケットモニタ手段と、前記パケットモニタ手段によりモニタされた少なくとも１個のパケットに含まれるＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）アドレスに基づいて、前記モニタされたパケットに関係するネットワーク機器に設定されたサブネットマスクを検出するサブネットマスク検出手段と、を有することを特徴とする。

【００１１】

前記サブネットマスク検出手段の第１形態は、前記モニタされた少なくとも１個のパケットに含まれる送信元ＩＰアドレスおよび送信先ＩＰアドレスの最大ＩＰアドレスと最小ＩＰアドレスとを求め、前記最大ＩＰアドレスおよび前記最小ＩＰアドレスのサブネットホスト部における異なるビットの最上位を特定することで前記サブネットマスクを検出することを特徴とする。

【００１２】

前記サブネットマスク検出手段の第２形態は、モニタされた複数のパケットの各々に含まれる送信元ＩＰアドレスおよび送信先ＩＰアドレスから各パケットのＩＰ領域を求め、前記モニタされた複数のパケットのＩＰ領域が重なる場合にはそれらを１つのＩＰ領域とし、最終的に求められた少なくとも１個のＩＰ領域から最大ＩＰアドレスと最小ＩＰアドレスとを求め、前記最大ＩＰアドレスおよび前記最小ＩＰアドレスのサブネットホスト部における異なるビットの最上位を特定することで前記サブネットマスクを検出することを特徴とする。

【００１３】

前記サブネットマスク検出手段の第３形態は、モニタされた１個のパケットに含まれるＩＰアドレスとネットワーク層で通信可能な他のＩＰアドレスの範囲を求め、当該ＩＰアドレス範囲に従って前記サブネットマスクを検出することを特徴とする。

【００１４】

本発明によれば、さらに、前記サブネットマスク検出手段により検出されたサブネットマスクにより示されるサブネット内のＩＰアドレスに対してＡＲＰ要求を送信し、ＡＲＰ応答が返信されないＩＰアドレスを割当可能なＩＰアドレスとして決定するＩＰアドレス決定手段を有することが望ましい。

【００１５】

本発明によれば、さらに、前記サブネットマスク検出手段により検出されたサブネットマスクにより示されるサブネット内のＩＰアドレスに対してＩＣＭＰエコー要求を順次送信し、それに対するＩＣＭＰ応答からルータのＩＰアドレスを検出するルータ検出手段を有することが望ましい。

本発明によれば、さらに、前記パケットモニタ手段によりモニタされたパケットに含まれる送信先ＩＰアドレスと送信先ＭＡＣアドレスとが同一のネットワーク機器を指示しない場合、当該送信先ＭＡＣアドレスに対応するＩＰアドレスをルータのＩＰアドレスとして検出するルータ検出手段を有することが望ましい。

【００１６】

本発明によれば、さらに、ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）のエコー要求およびエコー応答機能を用いて、モニタされたＩＰアドレスを使用している他のネットワーク機器のサブネットマスクと自己のサブネットマスクとの同一性を判定するサブネットマスク同一性判定手段を有し、前記他のネットワーク機器のサブネットマスクと前記自己のサブネットマスクとが異なる場合、前記サブネットマスク検出手段により当該他のネットワーク機器のサブネットマスクを検出することが望ましい。

【００１７】

本発明の他の側面によれば、ローカルネットワーク上のパケットをモニタするパケットモニタ手段と、前記パケットモニタ手段によりモニタされたパケットに含まれる送信先ＩＰアドレスと送信先ＭＡＣアドレスとが同一のネットワーク機器を指示しない場合、当該送信先ＭＡＣアドレスに対応するＩＰアドレスをルータのＩＰアドレスとして検出するルータ検出手段と、を有することを特徴とする。

【００１８】

本発明のさらに他の側面によれば、複数のネットワーク機器が接続されたローカルネットワークにおけるネットワーク情報を検出する方法において、ａ）前記ローカルネットワーク上のパケットをモニタするステップと、ｂ）モニタされたパケットのＩＰアドレス（以下、モニタＩＰアドレスという。）のネットワークアドレスと自己のネットワークアドレスとを比較するステップと、ｃ）ネットワークアドレスが同一の場合、ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）のエコー要求およびエコー応答機能を用いて、前記モニタＩＰアドレスを使用している他のネットワーク機器のサブネットマスクと自己のサブネットマスクとの同一性を判定するステップと、を有することを特徴とする。

【００１９】

【発明の実施の形態】
図１は本発明によるネットワーク情報検出装置を含むネットワークの一例を示す概略的構成図である。この例では、ネットワーク（ＬＡＮ）伝送路１０に、ネットワーク情報検出装置２０、ホストＡ３０、　ホストＢ４０、ホスト５０、および、ルータ６０などの複数のネットワーク機器が接続されている。本発明によるネットワーク情報検出装置２０は、後述するように、ネットワークで通信されるＩＰパケットやＡＲＰ（Ａｄｄｒｅｓｓ　Ｒｅｓｏｌｕｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）パケットを利用して、サブネットマスクの検出、ＩＰアドレスの決定、ルータの検出、あるいは、ネットワーク情報の設定などを実行する。

【００２０】
１．第１実施形態
図２は本発明の第１実施形態によるネットワーク情報検出装置を示すブロック構成図である。本実施形態によるネットワーク情報検出装置２０は、ネットワーク伝送路１０に接続するためのネットワークインタフェース部２１を有する。ネットワークインタフェース部２１はパケットモニタ２３、サブネットマスク検出部２４、ＩＰアドレス決定部２５、ルータ検出部２６、および、ネットワーク情報送信部２８に接続され、ＬＡＮ伝送路１０との間でＩＰパケットまたはＡＲＰパケットの送信または受信を行う。ネットワークインタフェース部２１は、ＬＡＮ　伝送路１０上の全てのパケットをパケットモニタ２３に流す。

【００２１】
パケットモニタ２３はサブネットマスク検出部２４に接続され、ネットワークインタフェース部２１から入力したＩＰパケットまたはＡＲＰパケットをモニタする。また、サブネットマスク検出部２４、ＩＰアドレス決定部２５、ルータ検出部２６およびネットワーク情報送信部２８はネットワーク情報設定部２７にそれぞれ接続されている。また、ネットワーク情報検出装置２０の全体的動作は制御部２２により制御される。

【００２２】
ＬＡＮ伝送路１０上を流れるパケットは、例えばＬＡＮがＥｔｈｅｒｎｅｔ（登録商標、ＩＥＥＥ８０２．３　）であれば、図３に示すフォーマットを有するデータリンク層のパケットであり、ＩＰパケットであれば図４に示すフォーマットを有し、ＡＲＰ　パケットであれば図５に示すフォーマットを有する。

【００２３】
サブネットマスク検出部２４は、パケットモニタ２３によりモニタされたＩＰパケットまたはＡＲＰパケットを解析し、当該パケットの送信元あるいは送信先ＩＰアドレスのホストに設定されたサブネットマスク情報の検出および／またはサブネットの判定を行う（詳しくは、図８～図１２を参照しながら詳述する）。なお、ＩＰアドレスの一般的な構成を図６に示しておく。

【００２４】
ＩＰアドレス決定部２５は、サブネットマスク検出部２４で検出したサブネットマスクにおいて未だ割り当てられていないＩＰアドレスを検出し、ネットワーク情報検出装置に設定すべきＩＰアドレスを決定する（詳しくは、図１３を参照しながら詳述する）。

【００２５】
ルータ検出部２６は、パケットモニタ２３でモニタしたＩＰパケットがルータ６０へ送信されるＩＰパケットの特徴を持っているか否かを判定してルータ６０を検出する（詳しくは、図１４～図１５を参照しながら詳述する）。あるいは、ルータ検出部２６は、サブネットマスク検出部２４で検出したサブネット内のＩＰアドレスに対して図７（Ａ）に示すフォーマットのＩＣＭＰ（Ｉｎｔｅｒｎｅｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ　Ｐｒｏｔｏｃｏｌ　）エコー要求を順次送信し、図７（Ｂ）に示すフォーマットのＩＣＭＰ時間切れメッセージ、あるいは、図７（Ｃ）に示すフォーマットのＩＣＭＰ経路変更要求メッセージを受信することによりルータ６０を検出する（詳しくは、図１６を参照しながら詳述する）。

【００２６】
ネットワーク情報設定部２７は、サブネットマスク検出部２４により検出したサブネットマスク、ＩＰアドレス決定部２５により検出した未割り当てＩＰアドレス、および、ルータ検出部２６により検出したルータＩＰアドレスの少なくとも１つからなるネットワーク情報を受け取り、自己の装置に設定するか、あるいは他の装置で利用可能とするためにネットワーク情報送信部２８に送信する。
【００２７】
ネットワーク情報送信部２８は、ネットワーク情報設定部２７から取得したネットワーク情報を他の装置で利用可能とするためにネットワークインタフェース部２１を通してＬＡＮ伝送路１０へ送出する。
【００２８】
ネットワーク情報検出動作
以下、本実施形態の動作を図３～図７に示すパケットフォーマットおよび図８～図１６に示すフローチャートを参照しながら詳細に説明する。
【００２９】
（１）サブネットマスク検出処理（第１例）
図８は、本実施形態におけるサブネットマスク検出処理の第１例を示すフローチャートである。まずパケットモニタ２３は、制御部２２の制御の下で、規定の時間、ＡＲＰパケットまたはＩＰパケットをモニタする（ステップＳ２４０１）。パケットの種類は、図３に示すように、イーサヘッダが含むタイプが０ｘ８０６であればＡＲＰパケット、０ｘ８００であればＩＰパケットであると判断される。規定時間内に一つ以上のＡＲＰまたはＩＰパケットをモニタした場合には（ステップＳ２４０２のＹＥＳ）、サブネットマスク検出部２４にモニタしたパケットを渡す。ＡＲＰパケットおよびＩＰパケットのいずれもモニタしなかった場合には（ステップＳ２４０２のＮＯ）、ステップＳ２４０１へ戻る。
【００３０】
サブネットマスク検出部２４は、パケットモニタ２３から受け取ったＩＰパケット（図４参照）あるいはＡＲＰパケット（図５参照）から送信元ＩＰアドレスおよび送信先ＩＰアドレスを読み出し、それらの最大値を最大ＩＰとし（ステップＳ２４０３）、最小値を最小ＩＰとして設定する（ステップＳ２４０４）。続いて、最大ＩＰと最小ＩＰとを比較し、値が異なる最上位ビットをサブネットのホスト部の最上位ビットとして設定する（ステップＳ２４０５）。そして、サブネットのホスト部の最上位ビット～最下位ビットをセットし、その他のビットをリセットして３２ビット値を計算し、その１の補数をとることでサブネットマスクを検出する（ステップＳ２４０６）。
【００３１】
例えば、最大ＩＰ＝“１０．５６．８８．５”、最小ＩＰ＝“１０．５６．８８．３”であった場合、下位８ビットは最大ＩＰで“０００００１０１”、最小ＩＰで“００００００１１”である。最大ＩＰおよび最小ＩＰの上位２４ビットは同一であるから、値の異なる最上位ビットは下線で示した最下位から３ビット目のビット２となり、サブネットのホスト部の最上位ビットはビット２であることがわかる。検出されたサブネットのホスト部の最上位ビット（ビット２）より上位のすべてのビットをリセットし、ビット２～ビット０までをセットすることで３２ビットの値“０．０．０．７”を得る。その１の補数を計算してサブネットマスク“２５５．２５５．２５５．２４８”＝“１１１１１１１１．１１１１１１１１．１１１１１１１１．１１１１０００”を得ることができる。
【００３２】
次に、一例として４個のＡＲＰまたはＩＰパケットをモニタした場合を取り上げ、サブネットマスク検出処理について具体的に説明する。
【００３３】
図９は、４個のＡＲＰまたはＩＰパケットをモニタした場合の各パケットが含むＩＰアドレスとＩＰ領域と示す模式図である。ここでは、ＡＲＰ／ＩＰパケットＮｏ．１～Ｎｏ．４がモニタされたものとする。図８に示すサブネットマスク検出処理によれば、ＩＰ領域

Ａがサブネットと判断される。ＩＰ領域Ａの最小ＩＰアドレスはＮｏ．１パケットの最小ＩＰアドレス、ＩＰ領域Ａの最大ＩＰアドレスはＮｏ４パケットの最大ＩＰアドレスとなる。

【００３４】

（２）サブネットマスク検出処理（第２例）

図１０は、本実施形態におけるサブネットマスク検出処理の第２例を示すフローチャートである。まずパケットモニタ２３は、制御部２２の制御の下で、規定の時間、ＡＲＰパケットまたはＩＰパケットをモニタする（ステップＳ２４１１）。規定時間内に２つ以上のＡＲＰまたはＩＰパケットをモニタした場合には（ステップＳ２４１２のＹＥＳ）、サブネットマスク検出部２４にモニタしたパケットを渡す。２つ以上のＡＲＰあるいはＩＰパケットをモニタしなかった場合には（ステップＳ２４１２のＮＯ）、ステップＳ２４０１へ戻る。

【００３５】

サブネットマスク検出部２４は、モニタされたパケットのそれぞれについて、送信元ＩＰアドレスおよび送信先ＩＰアドレスにより定まるＩＰ領域を検出し（ステップＳ２４１３）、続いて、これらＩＰ領域の重なりを検出する（ステップＳ２４１４～Ｓ２４１６）。

【００３６】

具体的には、あるＩＰ領域αの最大ＩＰアドレスをＭＡＸα，　最小ＩＰアドレスをＭＩＮαとすると、任意の２つのＩＰ領域ＡおよびＢに関して、ＭＩＮａ≦ＭＡＸｂ、かつ、ＭＡＸａ≧ＭＩＮｂという条件が満たされるか否かを判定する（ステップＳ２４１４）。この条件を満たす場合（ステップＳ２４１４のＹＥＳ）、ＩＰ領域ＡおよびＢを合わせて単一のＩＰ領域とする（ステップＳ２４１５）。例えば、ＩＰ領域ＡがＭＡＸａ＝“１９２．１６８．０．４０”、ＭＩＮａ＝“１９２．１６８．０．２０”、ＩＰ領域ＢがＭＡＸｂ＝“１９２．１６８．０．３０”、ＭＩＮｂ＝“１９２．１６８．０．１０”である場合、上記判定条件は満足されるから、ＩＰ領域ＡおよびＢはそれらを合わせた１つの新たなＩＰ領域と判断される。その結果、新たなＩＰ領域の最大ＩＰは“１９２．１６８．０．４０”、最小ＩＰは“１９２．１６８．０．１０”となる。

【００３７】

全てのＩＰ領域の組み合わせに関して上記重なり検出処理（ステップＳ２４１４～Ｓ２４１６）を繰り返し、重なり検出が完了すると（ステップＳ２４１６のＹＥＳ）、最終的に決定された少なくとも１つのＩＰ領域の最大値を最大ＩＰとし（ステップＳ２４１７）、最小値を最小ＩＰとして設定する（ステップＳ２４１８）。続いて、図８に示した第１例と同様に、最大ＩＰと最小ＩＰとを比較し、値が異なる最上位ビットをサブネットのホスト部の最上位ビットとして設定する（ステップＳ２４１９）。そして、サブネットのホスト部の最上位ビット～最下位ビットをセットし、その他のビットをリセットして３２ビット値を計算し、その１の補数をとることでサブネットマスクを検出する（ステップＳ２４２０）。上記ステップＳ２４１７～Ｓ２４２０をすべてのＩＰ領域についてサブネットマスクを検出するまで繰り返す（ステップＳ２４２１のＮＯ）。

【００３８】

すべてのＩＰ領域についてサブネットマスク検出が終了すると（ステップＳ２４２１のＹＥＳ）、サブネットマスク検出部２４は、検出されたサブネットマスクを用いてネットワーク部およびサブネット部が同一の値のサブネットを同一のサブネットと判断する（ステップＳ２４２２）。

【００３９】

このサブネットマスク検出処理の第２例を図９に示す４個のＡＲＰまたはＩＰパケットをモニタした場合に適用すると、次のようになる。すなわち、サブネットマスク検出部２４は、パケットＮｏ．２～Ｎｏ．４のＩＰ領域が重なっていることからこれらを１つのＩＰ領域Ｃと判定する。したがって、モニタされた４つのパケットに基づいて、サブネットマスク検出部２４はＩＰ領域ＢおよびＩＰ領域Ｃをそれぞれサブネットと判断する。図９に示すように、ＩＰ領域Ｂの最小ＩＰアドレスおよび最大ＩＰアドレスは、それぞれパケッ

トＮｏ．１の最小ＩＰアドレスおよび最大ＩＰアドレスとなる。ＩＰ領域Ｃの最小ＩＰアドレスはパケットＮｏ．２の最小ＩＰアドレス、最大ＩＰアドレスはパケットＮｏ．４の最大ＩＰアドレスとなる。

【００４０】

（３）サブネットマスク検出処理（第３例）

図１１は、本実施形態におけるサブネットマスク検出処理の第３例を示すフローチャートである。まずパケットモニタ２３は、制御部２２の制御の下で、ＡＲＰパケットまたはＩＰパケットをモニタする（ステップＳ２４４１）。ＡＲＰまたはＩＰパケットをモニタした場合には（ステップＳ２４４１のＹＥＳ）、サブネットマスク検出部２４にモニタしたパケットを渡す。

【００４１】

サブネットマスク検出部２４は、パケットモニタ２３から受け取ったモニタパケットから送信元ＩＰアドレスあるいは送信先ＩＰアドレスを読み出し、それをモニタＩＰとするとともに、そのモニタＩＰを検査ＩＰとし、ビットカウンタを０に設定し、セットビットを１に設定する（ステップＳ２４４２）。続いて、検査ＩＰとセットビットとのＯＲ（論理和）を計算して、その結果を検査ＩＰに設定するとともに、ビットカウンタに１を加算し、セットビットを１ビットだけ左シフトする（ステップＳ２４４３）。

【００４２】

続いて、サブネットマスク検出部２４は、送信元ＩＰアドレスに上記検査ＩＰを設定し、送信先ＩＰアドレスに上記モニタＩＰを設定したＩＣＭＰエコー要求（図７（Ａ）参照）を生成し、ネットワークインタフェース部２１を通してネットワークへ送信する（ステップＳ２４４４）。

【００４３】

ＩＣＭＰエコー要求パケットを送信すると、サブネットマスク検出部２４は、イーサヘッダの送信先ＭＡＣアドレスにブロードキャストアドレスを使用していないＩＣＭＰエコー応答（図７（Ａ）参照）を受信したか否かを判定する（ステップＳ２４４５）。受信したＩＣＭＰエコー応答が送信先ＭＡＣアドレスにブロードキャストアドレスを使用していない場合は（ステップＳ２４４５のＹＥＳ）、当該検査ＩＰアドレスとモニタアドレスとはＭＡＣアドレスにブロードキャストを使用することなくネットワーク層で通信可能であると判断し、ステップＳ２４４３へ戻る。

【００４４】

これに対して、イーサヘッダの送信先ＭＡＣアドレスにブロードキャストアドレスを使用していないＩＣＭＰエコー応答を受信しなかった場合には（ステップＳ２４４５のＮＯ）、ＭＡＣアドレスにブロードキャストを使用せずにネットワーク層で通信することができないと判断し、ビットカウンタから１を減算した値をビット番号Ａに設定し（ステップＳ２４４６）、ビットカウンタに０を設定し、リセットビットに１を設定する（ステップＳ２４４７）。

【００４５】

続いて、サブネットマスク検出部２４は、検査ＩＰとリセットビットの１の補数との論理積（ＡＮＤ）を計算し、その結果を検査ＩＰに設定するとともに、ビットカウンタに１を加算し、リセットビットを１ビットだけ左シフトする（ステップＳ２４４８）。

【００４６】

続いて、サブネットマスク検出部２４は、送信元ＩＰアドレスに上記検査ＩＰを設定し、送信先ＩＰアドレスに上記モニタＩＰを設定したＩＣＭＰエコー要求（図７（Ａ）参照）を生成し、ネットワークインタフェース部２１を通してネットワークへ送信する（ステップＳ２４４９）。

【００４７】

ＩＣＭＰエコー要求パケットを送信すると、サブネットマスク検出部２４は、イーサヘッダの送信先ＭＡＣアドレスにブロードキャストアドレスを使用していないＩＣＭＰエコー応答を受信したか否かを判定する（ステップＳ２４５０）。受信したＩＣＭＰエコー応答

が送信先ＭＡＣアドレスにブロードキャストアドレスを使用していない場合は（ステップＳ２４５０のＹＥＳ）、当該検査ＩＰアドレスとモニタアドレスとはＭＡＣアドレスにブロードキャストを使用することなくネットワーク層で通信可能であると判断し、ステップＳ２４４８へ戻る。

【００４８】

これに対して、イーサヘッダの送信先ＭＡＣアドレスにブロードキャストアドレスを使用していないＩＣＭＰエコー応答を受信しなかった場合には（ステップＳ２４５０のＮＯ）、ＭＡＣアドレスにブロードキャストを使用せずにネットワーク層で通信することができないと判断し、ビットカウンタから１を減算した値をビット番号Ｂに設定する（ステップＳ２４５１）。このビット番号Ｂをサブネットのホスト部の最上位ビット番号として設定する（ステップＳ２４５２）。

【００４９】

続いて、ビット番号Ａがビット番号Ｂより大きいか否か判定し（ステップＳ２４５３）、ビット番号Ａ＞ビット番号Ｂであった場合は（ステップＳ２４５３のＹＥＳ）、サブネットのホスト部の最上位ビット番号にビット番号Ａの値を設定し（ステップＳ２４５４）、ステップＳ２４５５を実行する。ビット番号Ａ≦ビット番号Ｂであった場合は（ステップＳ２４５３のＮＯ）、ステップＳ２４５４をスキップしてステップＳ２４５５を実行する。ステップＳ２４５５では、すでに述べたように、サブネットのホスト部の最上位ビット～最下位ビットをセットし、その他のビットをリセットして３２ビット値を計算し、その１の補数をとることでサブネットマスクを検出する。

【００５０】

上述したように、図１１に示すサブネットマスク検出処理では、モニタＩＰアドレスに基づいて検査ＩＰアドレスを順次生成し、生成された検査ＩＰアドレスとモニタＩＰアドレスとの間でブロードキャストアドレスを使用せずに通信可能であるか否かを判定することでサブネットの範囲を特定する。一例として、モニタされたＡＲＰ／ＩＰパケットの送信元あるいは送信先ＩＰアドレスに基づいて４個の検査ＩＰアドレスを生成してサブネットマスク検出を行う場合を説明する。

【００５１】

図１２は、４つの検査ＩＰアドレスを生成した場合のサブネットマスク検出処理を示す模式図である。ここでは、検査ＩＰアドレスＮｏ．１およびＮｏ．２が隣接したＩＰアドレスであり、検査ＩＰアドレスＮｏ．３およびＮｏ．４が隣接したＩＰアドレスであるとする。図１２には、モニタＩＰアドレスから検査ＩＰアドレスＮｏ．２およびＮｏ．３に対してＭＡＣアドレスにブロードキャストアドレスを使用しないＩＣＭＰエコー応答が返送され（通信ＯＫ）、検査ＩＰアドレスＮｏ．１およびＮｏ．４に対しては返送されなかった（通信ＮＧ）場合が示されている。

【００５２】

この場合、検査ＩＰアドレスＮｏ．１およびＮｏ．４は、サブネット内の最大または最小のＩＰアドレス、すなわち装置に割り当てることは出来ないブロードキャストアドレスであると判定される。言い換えれば、モニタＩＰアドレスと検査ＩＰアドレスＮｏ．２およびＮｏ．３との間はＭＡＣアドレスにブロードキャストアドレスを使用せずにネットワーク層で通信可能であるが、モニタＩＰアドレスと検査ＩＰアドレスＮｏ．１およびＮｏ．４との間はＭＡＣアドレスにブロードキャストアドレスを使用せずにネットワーク層で通信できず、従って、ＭＡＣアドレスにブロードキャストアドレスを使用せずにＩＣＭＰエコー通信も行えない。これにより、サブネットの範囲は検査ＩＰアドレスＮｏ．１～Ｎｏ．４で示す範囲であると判断される。

【００５３】

（４）割当可能ＩＰアドレス決定処理

上述したサブネットマスク検出処理によりサブネットマスクが検出されると、ＩＰアドレス決定部２５はサブネット内で割当可能なＩＰアドレスを決定する。

【００５４】

図１３は、ＩＰアドレス決定部２５における割当可能ＩＰアドレス決定処理を示すフローチャートである。まず、ＩＰアドレス決定部２５は、検査ＩＰアドレスにサブネット最小ＩＰアドレスを設定し（ステップＳ２５９１）、検査ＩＰアドレスに１を加算する（ステップＳ２５９２）。

【００５５】

続いて、ＩＰアドレス決定部２５は、検査ＩＰアドレスとサブネットの最大ＩＰアドレスとが等しいか否かを判定し（ステップＳ２５９３）、検査ＩＰアドレス＝サブネット最大ＩＰアドレスであれば（ステップＳ２５９３のＹＥＳ）、割り当て可能なＩＰアドレスは存在しないと判断して処理を終了する。検査ＩＰアドレスがサブネット最大ＩＰアドレスでない場合は（ステップＳ２５９３のＮＯ）、ターゲットＩＰアドレスを検査ＩＰアドレスとしたＡＲＰ要求を生成し、ネットワークインタフェース部２１を通してネットワーク１０へ送信する（ステップＳ２５９４）。

【００５６】

ＡＲＰ要求を送信すると、ＩＰアドレス決定部２５は、規定時間内に当該ＡＲＰ要求に対するＡＲＰ応答を受信したかどうかを判定し（ステップＳ２５９５）、受信した場合は（ステップＳ２５９５のＹＥＳ）、すでに割り当てられたＩＰアドレスであるから、ステップＳ２５９２へ戻って次のＩＰアドレスの検査を行う。規定時間内に当該ＡＲＰ要求に対するＡＲＰ応答を受信しなかった場合は（ステップＳ２５９５のＮＯ）、当該検査ＩＰアドレスはどのネットワーク装置にも割り当てられていないと判断され、ＩＰアドレス決定部２５はこのＩＰアドレスを割当て可能ＩＰアドレスとして決定する（ステップＳ２５９６）。

【００５７】

（５）ルータ検出処理（第１例）

図１４はルータ検出部２６におけるルータの検出動作の第１例を示すフローチャートである。パケットモニタ２３によりＩＰパケットがモニタされると（ステップＳ２６８１のＹＥＳ）、ルータ検出部２６は、当該モニタＩＰアドレスがサブネット外か否かを判断し（ステップＳ２６８２）、サブネット内であれば（ステップＳ２６８２のＮＯ）、ステップＳ２６８１に戻る。サブネット外か否かの判断については後述する。

【００５８】

当該モニタＩＰアドレスがサブネット外のアドレスであれば（ステップＳ２６８２のＹＥＳ）、ルータ検出部２６は当該モニタＩＰパケットの送信先ＭＡＣアドレスをルータのＭＡＣアドレスとして設定し（ステップＳ２６８３）、このルータＭＡＣアドレスをターゲットのハードウェアアドレスとしたＩｎＡＲＰ（Ｉｎｖｅｒｓｅ　Ａｄｄｒｅｓｓ　Ｒｅｓｏｌｕｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）要求をネットワークインタフェース部２１を通してネットワーク１０へ送信する（ステップＳ２６８４）。

【００５９】

ＩｎＡＲＰ要求を送信すると、ルータ検出部２６は、規定時間内にＩｎＡＲＰ応答を受信したか否かを判定する（ステップＳ２６８５）。規定時間内にＩｎＡＲＰ応答を受信しなかった場合は（ステップＳ２６８５のＮＯ）、ステップＳ２６８１へ戻る。規定時間内にＩｎＡＲＰ応答を受信した場合は（ステップＳ２６８５のＹＥＳ）、受信したＩｎＡＲＰ応答パケットに含まれる送信元プロトコルアドレスをルータのＩＰアドレスとして決定し（ステップＳ２６８６）、処理を終了する。

【００６０】

このようにサブネットの外部にあるホストへ送信されるＩＰパケットをモニタすることで当該サブネットのルータのＩＰアドレスを検出することができる。以下、図１５を用いてサブネットの外部へ送信されるＩＰパケットの特徴について説明する。

【００６１】

図１５は、サブネット外のネットワークに接続されたホストに送信するＩＰパケットの特徴を説明するためのネットワークを示す模式図である。同じサブネット内のホストＢからホストＡに送信するＩＰパケット（１）の場合、送信先ＩＰアドレスは当該ＩＰパケット

（１）を次に受信するホストＡのＩＰアドレスである。これに対して、ホストＢからサブネット外のネットワークに接続されたホストＺにＩＰパケット（２）を送信する場合、その送信先ＩＰアドレスは当該ＩＰパケットを次に受信するルータのＩＰアドレスではなく、外部のホストＺのＩＰアドレスである。したがって、ＩＰパケット（２）の送信先ＩＰアドレスはサブネット外のＩＰアドレスであると判断することができ、ルータのＭＡＣアドレスは当該ＩＰパケット（２）の送信先ＭＡＣアドレスであると判断される。したがって、ＩｎＡＲＰ要求および応答プロセスにより当該ルータのＩＰアドレスを検出することができる。

【００６２】

（６）ルータ検出処理（第２例）

図１６はルータ検出部２６におけるルータの検出動作の第２例を示すフローチャートである。まず、検査ＩＰアドレスにサブネット最小ＩＰアドレスを設定し（ステップＳ２６９１）、検査ＩＰアドレスに１を加算する（ステップＳ２６９２）。続いて、ルータ検出部２６は検査ＩＰアドレスとサブネット最大ＩＰアドレスとが等しいか否かを判定する（ステップＳ２６９３）。検査ＩＰアドレス＝サブネット最大ＩＰアドレスの場合には（ステップＳ２６９３のＹＥＳ）、サブネットにルータが存在しないと判断して処理を終了する。

【００６３】

検査ＩＰアドレスとサブネット最大ＩＰアドレスとが異なる場合には（ステップＳ２６９３のＮＯ）、検査ＩＰアドレスを送信先ＩＰアドレスに、所望の値をＴＴＬ（Ｔｉｍｅ Ｔｏ Ｌｉｖｅ）にそれぞれ設定したＩＣＭＰエコー要求パケット（図７（Ａ）参照）を送信する（ステップＳ２６９４）。ここでは、ＴＴＬ＝２、すなわち通過可能ルータ段数が２であるとする。

【００６４】

ＩＣＭＰエコー要求パケットを送信すると、ルータ検出部２６は、規定時間内に当該ＩＣＭＰエコー要求に対するＩＣＭＰ経路変更要求メッセージ（図７（Ｃ）参照）を受信したかどうかを判定する（ステップＳ２６９５）。

【００６５】

ＩＣＭＰ経路変更要求メッセージを受信しなかった場合は（ステップＳ２６９５のＮＯ）、規定時間内に当該ＩＣＭＰエコー要求に対するＩＣＭＰ時間切れメッセージ（図７（Ｂ））を受信したかどうかを判定する（ステップＳ２６９６）。ＩＣＭＰ時間切れメッセージを受信しなかった場合は（ステップＳ２６９６のＮｏ）、ステップＳ２６９２に戻る。規定時間内にＩＣＭＰ時間切れメッセージを受信した場合は（ステップＳ２６９６のＹＥＳ）、当該時間切れメッセージパケットが含む送信元ＩＰアドレスをルータのＩＰアドレスであると判断して（ステップＳ２６９７）、ルータ検出動作を終了する。

【００６６】

一方、ＩＣＭＰ経路変更要求メッセージを受信した場合は（ステップＳ２６９５のＹＥＳ）、当該経路変更要求メッセージが含むルータＩＰアドレスをルータのＩＰアドレスであると判断して（ステップＳ２６９８）、ルータ検出動作を終了する。このようにしてルータのＩＰアドレスを検出する。

【００６７】

上述したサブネットマスク検出処理、ＩＰアドレス決定処理、および、ルータ検出処理により、ネットワーク情報として、サブネットマスク、割り当て可能なＩＰアドレス、および、ルータＩＰアドレスをそれぞれ検出することができる。これらのネットワーク情報がネットワーク情報設定部２７へ出力される。

【００６８】

２．第２実施形態

図１７は本発明の第２実施形態によるネットワーク情報検出装置を示すブロック構成図である。本実施形態によるネットワーク情報検出装置２０は、制御部２２により制御されるサブネットマスク同一性判定部２９を有する点が図２に示す第１実施形態とは異なってい

る。したがって、ここでは第１実施形態と同じ構成および機能を有する回路ブロックには同じ参照番号２１～２８を付して説明は省略し、サブネットマスク同一性判定部２９の動作について詳細に説明する。

【００６９】

（１）サブネットマスク同一性検査（第１例）

図１８（Ａ）および（Ｂ）は、第２実施形態におけるサブネットマスク同一性検査方法の第１例を示すシーケンス図である。以下、説明を簡単にするために、サブネットマスク値の比較を行うネットワーク装置を「装置１」とし、比較対象となるネットワーク装置を「装置２」とする。

【００７０】

まず、図１８（Ａ）に示すように、装置１は、装置１あるいは装置２のＩＰアドレスのホスト部を０（すべて０）または－１（すべて１）としたＩＰアドレス（詳しくは後述する。）を送信元ＩＰアドレスとしたＩＣＭＰエコー要求を装置２へ送信する。装置１のサブネットマスクが装置２のそれよりも大きい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を返送し、装置１のサブネットマスクが装置２のそれ以下の場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を送信しないか、または、ブロードキャストで応答する。

【００７１】

ユニキャストのＩＣＭＰエコー応答がなかった場合には、図１８（Ｂ）に示すように、装置１は、装置２に対して、装置２のホスト部の各ビットを反転させたＩＰアドレスを送信元ＩＰアドレスとしたＩＣＭＰエコー要求を送信する。装置１のサブネットマスクが装置２のそれと等しい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を返送し、装置１のサブネットマスクが装置２のそれより小さい場合は、装置２は装置１にエコー応答を送信しない。

【００７２】

図１９は、本実施形態におけるサブネットマスク同一性検査動作の第１例を示すフローチャートである。このサブネットマスク同一性検査プロセスは、図１７におけるサブネットマスク同一性判定部２９により実行される。ここでは、図１８の「装置１」および「装置２」がそれぞれ「自装置」および「モニタＩＰアドレス使用装置」に対応する。

【００７３】

図１９において、まずパケットモニタ２３は、制御部２２の制御の下で、ＬＡＮ１０を流れるパケットをモニタし（ステップＳ３００１）、ＡＲＰパケットか否かを判定する（ステップＳ３００２）。ＡＲＰパケットでなければ（ステップＳ３００２のＮＯ）、続いてＩＰパケットか否かを判定する（ステップＳ３００３）。ＩＰパケットでもなければ（ステップＳ３００３のＮＯ）、ステップＳ３００１へ戻る。

【００７４】

モニタされたパケットがＩＰパケットである場合には（ステップＳ３００３のＹＥＳ）、サブネットマスク同一性判定部２９は、送信元ＩＰアドレスを自装置のＩＰアドレスに、送信先ＩＰアドレスをモニタＩＰアドレスにそれぞれ設定したＡＲＰ要求を生成して送信し（ステップＳ３００４）、その応答を待つ。

【００７５】

規定時間内に当該ＡＲＰ要求に対するＡＲＰ応答がなければ（ステップＳ３００５のＮＯ）、当該モニタＩＰアドレスはＬＡＮ１０の外部にあると判断され、ステップＳ３００１へ戻る。

【００７６】

規定時間内に当該ＡＲＰ要求に対するＡＲＰ応答を受信した場合（ステップＳ３００５のＹＥＳ）、あるいは、ステップＳ３００２においてＡＲＰパケットをモニタした場合には（ステップＳ３００２のＹＥＳ）、サブネットマスク同一性判定部２９は、当該モニタＩＰアドレスはＬＡＮ１０の内部にあると判断し、当該モニタＩＰアドレスのネットワークアドレス（ネットワーク部＋サブネット部）と自装置のそれとが等しいか否かを判断する

（ステップＳ３００６）。モニタＩＰアドレスのネットワークアドレスと自装置のそれとが異なる場合には（ステップＳ３００６のＮＯ）、この検査処理を終了する。

【００７７】

モニタＩＰアドレスのネットワークアドレスと自装置のそれとが等しい場合は（ステップＳ３００６のＹＥＳ）、自装置のＩＰアドレスまたはモニタＩＰアドレスのホスト部を０または－１とした値を送信元ＩＰアドレスとし、モニタＩＰアドレスを送信先ＩＰアドレスとしたＩＣＭＰエコー要求を生成して送信する（ステップＳ３００７）。ここで、ホスト部を０にするとはホスト部の全てのビットを０にすることであり、ホスト部を－１にするとは全てのビットを１にすることである。ホスト部を０にするのは自装置ＩＰアドレスのネットワークアドレスのＬＳＢが１の場合であり、ホスト部を－１にするのは自装置ＩＰアドレスのネットワークアドレスのＬＳＢが０の場合である。例えば、自装置のＩＰアドレスが“１０．５６．８８．１”、サブネットマスクが“２５５．２５５．２５５．０”の場合には、ＩＣＭＰエコー要求の送信元ＩＰアドレスは“１０．５６．８８．２５５”に設定される。自装置のＩＰアドレスが“１０．５６．８９．１”、サブネットマスクが“２５５．２５５．２５５．０”の場合には、ＩＣＭＰエコー要求の送信元ＩＰアドレスは“１０．５６．８９．０”に設定される。

【００７８】

ＩＣＭＰエコー要求を送信すると、サブネットマスク同一性判定部２９は、モニタＩＰアドレスの装置（モニタＩＰアドレス使用装置）からユニキャストのＩＣＭＰエコー応答があったか否かを判断する（ステップＳ３００８）。

【００７９】

ユニキャストのＩＣＭＰエコー応答がなかった場合には（ステップＳ３００８のＮＯ）、サブネットマスク同一性判定部２９は、モニタＩＰアドレスのホスト部の各ビットを反転した値を送信元ＩＰアドレスに、モニタＩＰアドレスを送信先ＩＰアドレスにそれぞれ設定したＩＣＭＰエコー要求を生成して送信する（ステップＳ３００９）。ここで、ＩＣＭＰエコー要求の送信元ＩＰアドレスは、モニタＩＰアドレスのホスト部の最上位ビット（ＭＳＢ）を反転し、他のビットはホスト部全体が０または－１とならないどんな値でも良い。例えば、モニタＩＰアドレスが“１０．５６．８８．２”、自装置のサブネットマスクが“２５５．２５５．２５５．０”の場合には、ＩＣＭＰエコー要求の送信元ＩＰアドレスは“１０．５６．８８．２５４”～“１０．５６．８８．１２８”のどれでもよい。

【００８０】

続いて、サブネットマスク同一性判定部２９は、このＩＣＭＰエコー要求に対してモニタＩＰアドレス使用装置からユニキャストのエコー応答があったか否かを判断する（ステップＳ３０１０）。ユニキャストのエコー応答があった場合は（ステップＳ３０１０のＹＥＳ）、自装置のサブネットマスク値がモニタＩＰアドレス使用装置のそれよりも小さいと判定し（ステップＳ３０１１）、処理を終了する。逆に、ユニキャストのエコー応答がなかった場合は（ステップＳ３０１０のＮＯ）、自装置のサブネットマスク値とモニタＩＰアドレス使用装置のそれとが等しいと判定し（ステップＳ３０１３）、処理を終了する。

【００８１】

また、ステップＳ３００８において、ユニキャストのＩＣＭＰエコー応答があった場合には（ステップＳ３００８のＹＥＳ）、自装置のサブネットマスク値がモニタＩＰアドレス使用装置のそれよりも大きいと判定し（ステップＳ３０１２）、処理を終了する。

【００８２】

このように、二つの装置で使用するサブネットマスクの同一性を検証することができる。そして、これらのサブネットマスクが異なると判定された場合には、制御部２２は、サブネットマスク検出部２４、ＩＰアドレス決定部２５、および、ルータ検出部２６を制御して、上述したように、所望のサブネットマスク、未割り当てＩＰアドレスおよびルータＩＰアドレスの検出、これらネットワーク情報のネットワーク情報設定部２７への転送、ネットワーク情報設定部２７からネットワーク情報送信部２８への転送、および、ネットワーク情報送信部２８からネットワークインタフェース部２１への転送を、必要に応じて選

択的に実行あるいは再実行する。

【００８３】

また、サブネットマスクが異なると判定されたネットワーク機器またはネットワークアドレスが異なると判定されたネットワーク機器に対して、電子メールなどの通信手段を通してネットワークアドレスやサブネットマスクの設定が間違っている旨を通知してもよい。その際、ネットワークアドレスやサブネットマスクを自動設定するために、必要なネットワーク情報をネットワーク情報送信部２８から送信してもよい。

【００８４】

（２）サブネットマスク同一性検査（第２例）

図２０（Ａ）および（Ｂ）は、第２実施形態におけるサブネットマスク同一性検査方法の第２例を示すシーケンス図である。以下、説明を簡単にするために、サブネットマスク値の比較を行うネットワーク装置を「装置１」とし、比較対象となるネットワーク装置を「装置２」とする。

【００８５】

まず、図２０（Ａ）に示すように、装置１は、装置２に対して、装置２のホスト部の各ビットを反転させたＩＰアドレスを送信元ＩＰアドレスとしたＩＣＭＰエコー要求を送信する。装置１のサブネットマスクが装置２のそれ以上の場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を返送し、装置１のサブネットマスクが装置２のそれより小さい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を送信しない。

【００８６】

ユニキャストのＩＣＭＰエコー応答があった場合には、図２０（Ｂ）に示すように、装置１は、装置１あるいは装置２のＩＰアドレスのホスト部を０（すべて０）または－１（すべて１）としたＩＰアドレスを送信元ＩＰアドレスとしたＩＣＭＰエコー要求を装置２へ送信する。装置１のサブネットマスクが装置２のそれよりも大きい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を返送し、装置１のサブネットマスクと装置２のそれが等しい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を送信しないか、または、ブロードキャストで応答する。

【００８７】

図２１は、本実施形態におけるサブネットマスク同一性検査動作の第２例を示すフローチャートである。このサブネットマスク同一性検査プロセスは、図１７におけるサブネットマスク同一性判定部２９により実行される。ここでは、図２０の「装置１」および「装置２」がそれぞれ「自装置」および「モニタＩＰアドレス使用装置」に対応する。なお、図２１において、ステップＳ４００１～Ｓ４００６は、図１９のステップＳ３００１～Ｓ３００６にそれぞれ対応するので、説明は省略する。

【００８８】

ステップＳ４００６において、モニタＩＰアドレスのネットワークアドレスと自装置のそれとが等しい場合は（ステップＳ４００６のＹＥＳ）、サブネットマスク同一性判定部２９は、モニタＩＰアドレスのホスト部の各ビットを反転した値を送信元ＩＰアドレスに、モニタＩＰアドレスを送信先ＩＰアドレスにそれぞれ設定したＩＣＭＰエコー要求を生成して送信する（ステップＳ４００７）。ここで、ＩＣＭＰエコー要求の送信元ＩＰアドレスは、モニタＩＰアドレスのホスト部の最上位ビット（ＭＳＢ）を反転し、他のビットはホスト部全体が０または－１とならないどんな値でも良い。例えば、モニタＩＰアドレスが“１０．５６．８８．２”、自装置のサブネットマスクが“２５５．２５５．２５５．０”の場合には、ＩＣＭＰエコー要求の送信元ＩＰアドレスは“１０．５６．８８．２５４”～“１０．５６．８８．１２８”のどれでもよい。

【００８９】

ＩＣＭＰエコー要求を送信すると、サブネットマスク同一性判定部２９は、モニタＩＰアドレスの装置（モニタＩＰアドレス使用装置）からユニキャストのＩＣＭＰエコー応答があったか否かを判断する（ステップＳ４００８）。

【００９０】

ユニキャストのＩＣＭＰエコー応答があった場合には（ステップＳ４００８のＹＥＳ）、サブネットマスク同一性判定部２９は、自装置のＩＰアドレスまたはモニタＩＰアドレスのホスト部を０または－１とした値を送信元ＩＰアドレスとし、モニタＩＰアドレスを送信先ＩＰアドレスとしたＩＣＭＰエコー要求を生成して送信する（ステップＳ４００９）。ここで、ホスト部を０にするとは、上述したように、ホスト部の全てのビットを０にすることであり、ホスト部を－１にするとは全てのビットを１にすることである。また、ホスト部を０にするのは自装置ＩＰアドレスのネットワークアドレスのＬＳＢが１の場合であり、ホスト部を－１にするのは自装置ＩＰアドレスのネットワークアドレスのＬＳＢが０の場合である。

【００９１】

続いて、サブネットマスク同一性判定部２９は、このＩＣＭＰエコー要求に対してモニタＩＰアドレス使用装置からユニキャストのエコー応答があったか否かを判断する（ステップＳ４０１０）。ユニキャストのエコー応答があった場合は（ステップＳ４０１０のＹＥＳ）、自装置のサブネットマスク値がモニタＩＰアドレス使用装置のそれよりも大きいと判定し（ステップＳ４０１１）、処理を終了する。逆に、ユニキャストのエコー応答がなかった場合は（ステップＳ４０１０のＮＯ）、自装置のサブネットマスク値とモニタＩＰアドレス使用装置のそれとが等しいと判定し（ステップＳ４０１３）、処理を終了する。

【００９２】

また、ステップＳ４００８において、ユニキャストのＩＣＭＰエコー応答がなかった場合には（ステップＳ４００８のＮＯ）、自装置のサブネットマスク値がモニタＩＰアドレス使用装置のそれよりも小さいと判定し（ステップＳ４０１２）、処理を終了する。

【００９３】

このように、二つの装置で使用するサブネットマスクの同一性を検証することができる。そして、これらのサブネットマスクが異なると判定された場合には、制御部２２は、サブネットマスク検出部２４、ＩＰアドレス決定部２５、および、ルータ検出部２６を制御して、上述したように、所望のサブネットマスク、未割り当てＩＰアドレスおよびルータＩＰアドレスの検出、これらネットワーク情報のネットワーク情報設定部２７への転送、ネットワーク情報設定部２７からネットワーク情報送信部２８への転送、および、ネットワーク情報送信部２８からネットワークインタフェース部２１への転送を、必要に応じて選択的に実行あるいは再実行する。

【００９４】

また、サブネットマスクが異なると判定されたネットワーク機器またはネットワークアドレスが異なると判定されたネットワーク機器に対して、電子メールなどの通信手段を通してネットワークアドレスやサブネットマスクの設定が間違っている旨を通知してもよい。その際、ネットワークアドレスやサブネットマスクを自動設定するために、必要なネットワーク情報をネットワーク情報送信部２８から送信してもよい。

【００９５】

（３）サブネットマスク同一性検査（第３例）

図２２（Ａ）および（Ｂ）は、第２実施形態におけるサブネットマスク同一性検査方法の第３例を示すシーケンス図である。以下、説明を簡単にするために、サブネットマスク値の比較を行うネットワーク装置を「装置１」とし、比較対象となるネットワーク装置を「装置２」とする。

【００９６】

まず、図２２（Ａ）に示すように、装置１は、装置２に対して、装置２のホスト部の各ビットを反転させたＩＰアドレスを送信元ＩＰアドレスとしたＩＣＭＰエコー要求を送信する。装置１のサブネットマスクが装置２のそれ以上の場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を返送し、装置１のサブネットマスクが装置２のそれより小さい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を送信しない。

【００９７】

ユニキャストのＩＣＭＰエコー応答があった場合には、図２２（Ｂ）に示すように、装置

１は、装置１あるいは装置２のＩＰアドレスにおけるネットワークアドレスのＬＳＢを反転したものを送信元ＩＰアドレスとしたＩＣＭＰエコー要求を装置２へ送信する。装置１のサブネットマスクが装置２のそれよりも大きい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を返送し、装置１のサブネットマスクと装置２のそれが等しい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を送信しない。

【００９８】

図２３は、本実施形態におけるサブネットマスク同一性検査動作の第３例を示すフローチャートである。このサブネットマスク同一性検査プロセスは、図１７におけるサブネットマスク同一性判定部２９により実行される。ここでは、図２２の「装置１」および「装置２」がそれぞれ「自装置」および「モニタＩＰアドレス使用装置」に対応する。なお、図２３において、ステップＳ５００１～Ｓ５００６は、図１９のステップＳ３００１～Ｓ３００６にそれぞれ対応するので、説明は省略する。

【００９９】

ステップＳ５００６において、モニタＩＰアドレスのネットワークアドレスと自装置のそれとが等しい場合は（ステップＳ５００６のＹＥＳ）、サブネットマスク同一性判定部２９は、モニタＩＰアドレスのホスト部の各ビットを反転した値を送信元ＩＰアドレスに、モニタＩＰアドレスを送信先ＩＰアドレスにそれぞれ設定したＩＣＭＰエコー要求を生成して送信する（ステップＳ５００７）。ここで、ＩＣＭＰエコー要求の送信元ＩＰアドレスは、モニタＩＰアドレスのホスト部の最上位ビット（ＭＳＢ）を反転し、他のビットはホスト部全体が０または－１とならないどんな値でも良い。例えば、モニタＩＰアドレスが“１０．５６．８８．２”、自装置のサブネットマスクが“２５５．２５５．２５５．０”の場合には、ＩＣＭＰエコー要求の送信元ＩＰアドレスは“１０．５６．８８．２５４”～“１０．５６．８８．１２８”のどれでもよい。

【０１００】

ＩＣＭＰエコー要求を送信すると、サブネットマスク同一性判定部２９は、モニタＩＰアドレスの装置（モニタＩＰアドレス使用装置）からユニキャストのＩＣＭＰエコー応答があったか否かを判断する（ステップＳ５００８）。

【０１０１】

ユニキャストのＩＣＭＰエコー応答があった場合には（ステップＳ５００８のＹＥＳ）、自装置ＩＰアドレスまたはモニタＩＰアドレスにおける自装置のサブネットマスクが示すネットワークアドレスのＬＳＢを反転した値を送信元ＩＰアドレスとし、モニタＩＰアドレスを送信先ＩＰアドレスとしたＩＣＭＰエコー要求を生成して送信する（ステップＳ５００９）。

【０１０２】

続いて、サブネットマスク同一性判定部２９は、このＩＣＭＰエコー要求に対してモニタＩＰアドレス使用装置からユニキャストのエコー応答があったか否かを判断する（ステップＳ５０１０）。ユニキャストのエコー応答があった場合は（ステップＳ５０１０のＹＥＳ）、自装置のサブネットマスク値がモニタＩＰアドレス使用装置のそれよりも大きいと判定し（ステップＳ５０１１）、処理を終了する。逆に、ユニキャストのエコー応答がなかった場合は（ステップＳ５０１０のＮＯ）、自装置のサブネットマスク値とモニタＩＰアドレス使用装置のそれとが等しいと判定し（ステップＳ５０１３）、処理を終了する。

【０１０３】

また、ステップＳ５００８において、ユニキャストのＩＣＭＰエコー応答がなかった場合には（ステップＳ５００８のＮＯ）、自装置のサブネットマスク値がモニタＩＰアドレス使用装置のそれよりも小さいと判定し（ステップＳ５０１２）、処理を終了する。

【０１０４】

このように、二つの装置で使用するサブネットマスクの同一性を検証することができる。そして、これらのサブネットマスクが異なると判定された場合には、制御部２２は、サブネットマスク検出部２４、ＩＰアドレス決定部２５、および、ルータ検出部２６を制御して、上述したように、所望のサブネットマスク、未割り当てＩＰアドレスおよびルータＩ

Ｐアドレスの検出、これらネットワーク情報のネットワーク情報設定部２７への転送、ネットワーク情報設定部２７からネットワーク情報送信部２８への転送、および、ネットワーク情報送信部２８からネットワークインタフェース部２１への転送を、必要に応じて選択的に実行あるいは再実行する。

【０１０５】

また、サブネットマスクが異なると判定されたネットワーク機器またはネットワークアドレスが異なると判定されたネットワーク機器に対して、電子メールなどの通信手段を通してネットワークアドレスやサブネットマスクの設定が間違っている旨を通知してもよい。その際、ネットワークアドレスやサブネットマスクを自動設定するために、必要なネットワーク情報をネットワーク情報送信部２８から送信してもよい。

【０１０６】

（４）サブネットマスク同一性検査（第４例）

図２４（Ａ）および（Ｂ）は、第２実施形態におけるサブネットマスク同一性検査方法の第４例を示すシーケンス図である。以下、説明を簡単にするために、サブネットマスク値の比較を行うネットワーク装置を「装置１」とし、比較対象となるネットワーク装置を「装置２」とする。

【０１０７】

まず、図２４（Ａ）に示すように、装置１は、装置１あるいは装置２のＩＰアドレスにおけるネットワークアドレスのＬＳＢを反転したものを送信元ＩＰアドレスとしたＩＣＭＰエコー要求を装置２へ送信する。装置１のサブネットマスクが装置２のそれよりも大きい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を返送し、装置１のサブネットマスクが装置２のそれ以下の場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を送信しない。

【０１０８】

ユニキャストのＩＣＭＰエコー応答がなかった場合には、図２４（Ｂ）に示すように、装置１は、装置２に対して、装置２のホスト部の各ビットを反転させたＩＰアドレスを送信元ＩＰアドレスとしたＩＣＭＰエコー要求を送信する。装置１のサブネットマスクと装置２のそれとが等しい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を返送し、装置１のサブネットマスクが装置２のそれより小さい場合は、装置２は装置１にユニキャストのＩＣＭＰエコー応答を送信しない。

【０１０９】

図２５は、本実施形態におけるサブネットマスク同一性検査動作の第４例を示すフローチャートである。このサブネットマスク同一性検査プロセスは、図１７におけるサブネットマスク同一性判定部２９により実行される。ここでは、図２４の「装置１」および「装置２」がそれぞれ「自装置」および「モニタＩＰアドレス使用装置」に対応する。なお、図２５において、ステップＳ６００１～Ｓ６００６は、図１９のステップＳ３００１～Ｓ３００６にそれぞれ対応するので、説明は省略する。

【０１１０】

ステップＳ６００６において、モニタＩＰアドレスのネットワークアドレスと自装置のそれとが等しい場合は（ステップＳ６００６のＹＥＳ）、自装置ＩＰアドレスまたはモニタＩＰアドレスにおける自装置のサブネットマスクが示すネットワークアドレスのＬＳＢを反転した値を送信元ＩＰアドレスとし、モニタＩＰアドレスを送信先ＩＰアドレスとしたＩＣＭＰエコー要求を生成して送信する（ステップＳ６００７）。

【０１１１】

ＩＣＭＰエコー要求を送信すると、サブネットマスク同一性判定部２９は、モニタＩＰアドレスの装置（モニタＩＰアドレス使用装置）からユニキャストのＩＣＭＰエコー応答があったか否かを判断する（ステップＳ６００８）。

【０１１２】

ユニキャストのＩＣＭＰエコー応答がなかった場合には（ステップＳ６００８のＮＯ）、サブネットマスク同一性判定部２９は、モニタＩＰアドレスのホスト部の各ビットを反転

した値を送信元ＩＰアドレスに、モニタＩＰアドレスを送信先ＩＰアドレスにそれぞれ設定したＩＣＭＰエコー要求を生成して送信する（ステップＳ６００９）。ここで、ＩＣＭＰエコー要求の送信元ＩＰアドレスは、モニタＩＰアドレスのホスト部の最上位ビット（ＭＳＢ）を反転し、他のビットはホスト部全体が０または－１とならないどんな値でも良い。例えば、モニタＩＰアドレスが“１０．５６．８８．２”、自装置のサブネットマスクが“２５５．２５５．２５５．０”の場合には、ＩＣＭＰエコー要求の送信元ＩＰアドレスは“１０．５６．８８．２５４”～“１０．５６．８８．１２８”のどれでもよい。

【０１１３】

続いて、サブネットマスク同一性判定部２９は、このＩＣＭＰエコー要求に対してモニタＩＰアドレス使用装置からユニキャストのエコー応答があったか否かを判断する（ステップＳ６０１０）。ユニキャストのエコー応答があった場合は（ステップＳ６０１０のＹＥＳ）、自装置のサブネットマスク値とモニタＩＰアドレス使用装置のそれとが等しいと判定し（ステップＳ６０１１）、処理を終了する。逆に、ユニキャストのエコー応答がなかった場合は（ステップＳ６０１０のＮＯ）、自装置のサブネットマスク値はモニタＩＰアドレス使用装置のそれより小さいと判定し（ステップＳ６０１３）、処理を終了する。

【０１１４】

また、ステップＳ６００８において、ユニキャストのＩＣＭＰエコー応答があった場合には（ステップＳ６００８のＹＥＳ）、自装置のサブネットマスク値がモニタＩＰアドレス使用装置のそれよりも大きいと判定し（ステップＳ６０１２）、処理を終了する。

【０１１５】

このように、二つの装置で使用するサブネットマスクの同一性を検証することができる。そして、これらのサブネットマスクが異なると判定された場合には、制御部２２は、サブネットマスク検出部２４、ＩＰアドレス決定部２５、および、ルータ検出部２６を制御して、上述したように、所望のサブネットマスク、未割り当てＩＰアドレスおよびルータＩＰアドレスの検出、これらネットワーク情報のネットワーク情報設定部２７への転送、ネットワーク情報設定部２７からネットワーク情報送信部２８への転送、および、ネットワーク情報送信部２８からネットワークインタフェース部２１への転送を、必要に応じて選択的に実行あるいは再実行する。

【０１１６】

また、サブネットマスクが異なると判定されたネットワーク機器またはネットワークアドレスが異なると判定されたネットワーク機器に対して、電子メールなどの通信手段を通してネットワークアドレスやサブネットマスクの設定が間違っている旨を通知してもよい。その際、ネットワークアドレスやサブネットマスクを自動設定するために、必要なネットワーク情報をネットワーク情報送信部２８から送信してもよい。

【０１１７】

３．第３実施形態

図２６は本発明の第３実施形態によるネットワーク情報検出装置を示すブロック構成図である。本実施形態によるネットワーク情報検出装置２０は、ネットワーク伝送路１０に接続するためのネットワークインタフェース２０１と、上述したＩＰパケットあるいはＡＲＰパケットを送受信するための送受信制御部２０２とを有し、プログラム制御プロセッサ２０３が上述したネットワーク情報の検出、決定、設定などの処理を制御する。

【０１１８】

プログラム制御プロセッサ２０３は、プログラムメモリ２０４に格納されたサブネットマスク検出プログラム、ＩＰアドレス決定プログラム、ルータ検出プログラム、および、サブネットマスク同一性判定プログラムをそれぞれ読み出して実行することにより、上述したネットワーク情報検出動作、すなわちサブネットマスク検出、ＩＰアドレス決定およびルータ検出の処理、さらにサブネットマスク同一性判定の処理を行うことができる。こうして検出されたネットワーク情報はネットワーク情報メモリ２０５に格納され、自装置へ設定される。あるいは、ネットワーク上の他の装置の設定のために送信される。

【０１１９】

なお、本発明は、上述実施例に限定されるものではなく、発明の趣旨に沿って種々変形して適用することが可能である。検出するネットワーク情報は上記説明に挙げた全てである必要はなく、必要に応じて該当機能を実装すれば良い。また、ＩＰアドレス決定部あるいはネットワーク情報送信部の一方のみを実装した構成も考えられる。

【０１２０】

【発明の効果】

以上詳細に説明したように、　本発明によれば、サブネット外部のＩＰアドレスを使用せずに、ネットワークで使用しているサブネットマスク情報を取得することが可能となる。サブネット外部のＩＰアドレスを使用しないことで、サブネット外部にパケットを送信する必要がなくなる。これにより、サブネット外部にそのＩＰアドレスを使用するネットワーク装置が存在する場合であっても、当該ネットワーク装置へＩＰパケット送信して正常動作を阻害する可能性を排除できる。

【０１２１】

また検出したサブネットから、未割り当てのＩＰアドレスを決定し、さらにルータのＩＰアドレスを検出するという処理を自動で行い、ネットワーク装置を自動設定することができる。このため、ユーザの手作業でのネットワーク情報の入力作業を無くし、また間違えて入力した場合のネットワークの混乱を防ぐ効果がある。

【０１２２】

さらに、販売店で購入してきたネットワーク装置をユーザのネットワークに接続するだけで、特別なネットワーク情報設定操作をする必要がなく、他のネットワーク装置とネットワーク層での通信が可能となる。

【０１２３】

またネットワーク装置を他のネットワークに移動した場合にも、ネットワーク情報を人手で設定をすること無く、他のネットワーク装置とネットワーク層で通信可能となる効果がある。

【０１２４】

さらに、本発明によればネットワークアドレスやサブネットマスクの同一性を判定することができるために、モニタされたＩＰアドレスを使用するネットワーク機器の管理者に、メール、専用アプリケーションソフト、専用装置あるいは口頭でネットワークアドレスやサブネットマスクの設定が間違っている旨を通知し、自動でネットワークアドレスやサブネットマスクを設定することができる。

【図面の簡単な説明】

【図１】本発明によるネットワーク情報検出装置を含むネットワークの一例を示す概略的構成図である。

【図２】本発明の第１実施形態によるネットワーク情報検出装置を示すブロック構成図である。

【図３】イーサネット（登録商標）パケットのフォーマットを示す図である。

【図４】ＩＰパケットのフォーマットを示す図である。

【図５】ＡＲＰパケットのフォーマットを示す図である。

【図６】ＩＰアドレスのフォーマットを示す図である。

【図７】（Ａ）はＩＣＭＰエコー要求／応答パケットのフォーマットを示す図、（Ｂ）はＩＣＭＰ時間切れ通知パケットのフォーマットを示す図、（Ｃ）はＩＣＭＰ経路変更要求パケットのフォーマットを示す図である。

【図８】本実施形態におけるサブネットマスク検出処理の第１例を示すフローチャートである。

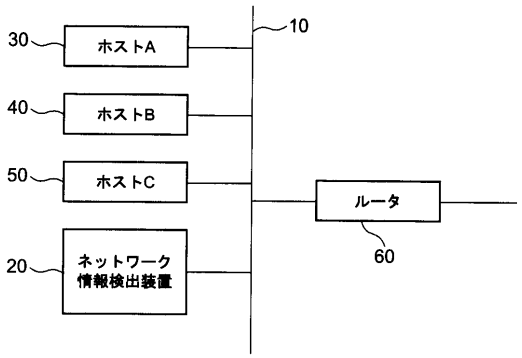
【図９】４個のＡＲＰまたはＩＰパケットをモニタした場合の各パケットが含むＩＰアドレスとＩＰ領域と示す模式図である。

【図１０】本実施形態におけるサブネットマスク検出処理の第２例を示すフローチャートである。

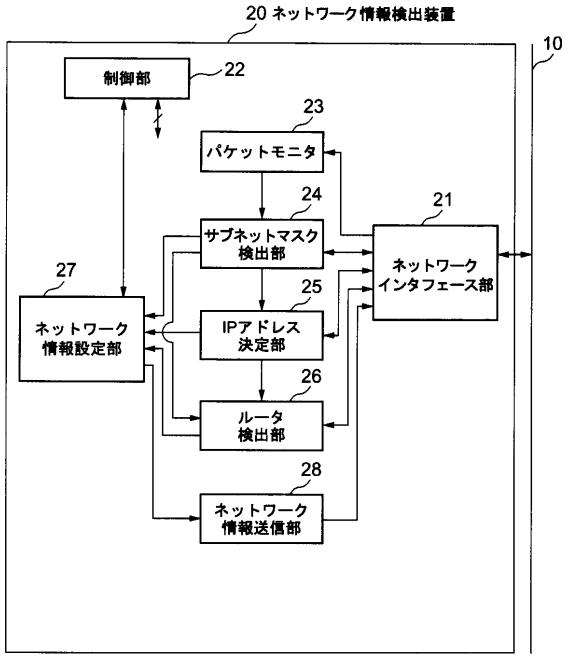
【図１１】本実施形態におけるサブネットマスク検出処理の第３例を示すフローチャート

である。
【図１２】４つの検査ＩＰアドレスを生成した場合のサブネットマスク検出処理を示す模式図である。
【図１３】ＩＰアドレス決定部２５における割当可能ＩＰアドレス決定処理を示すフローチャートである。
【図１４】ルータ検出部２６におけるルータの検出動作の第１例を示すフローチャートである。
【図１５】サブネット外のネットワークに接続されたホストに送信するＩＰパケットの特徴を説明するためのネットワークを示す模式図である。
【図１６】ルータ検出部２６におけるルータの検出動作の第２例を示すフローチャートである。
【図１７】本発明の第２実施形態によるネットワーク情報検出装置を示すブロック構成図である。
【図１８】（Ａ）および（Ｂ）は、第２実施形態におけるサブネットマスク同一性検査方法の第１例を示すシーケンス図である。
【図１９】本実施形態におけるサブネットマスク同一性検査動作の第１例を示すフローチャートである。
【図２０】（Ａ）および（Ｂ）は、第２実施形態におけるサブネットマスク同一性検査方法の第２例を示すシーケンス図である。
【図２１】本実施形態におけるサブネットマスク同一性検査動作の第２例を示すフローチャートである。
【図２２】（Ａ）および（Ｂ）は、第２実施形態におけるサブネットマスク同一性検査方法の第３例を示すシーケンス図である。
【図２３】本実施形態におけるサブネットマスク同一性検査動作の第３例を示すフローチャートである。
【図２４】（Ａ）および（Ｂ）は、第２実施形態におけるサブネットマスク同一性検査方法の第４例を示すシーケンス図である。
【図２５】本実施形態におけるサブネットマスク同一性検査動作の第４例を示すフローチャートである。
【図２６】本発明の第３実施形態によるネットワーク情報検出装置を示すブロック構成図である。
【符号の説明】
１０　ＬＡＮ伝送路
２０　ネットワーク情報検出装置
２１　ネットワークインタフェース部
２２　制御部
２３　パケットモニタ
２４　サブネットマスク検出部
２５　ＩＰアドレス決定部
２６　ルータ検出部
２７　ネットワーク情報設定部
２８　ネットワーク情報送信部
２９　サブネットマスク同一性判定部
３０～５０　ホスト
６０　ルータ

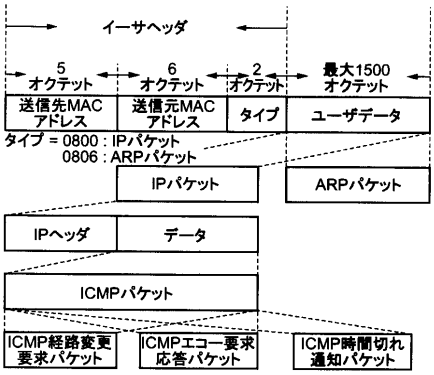
【図１】


30
ホストA
40
ホストB
50
ホストC
20
ネットワーク
情報検出装置
10
ルータ
60

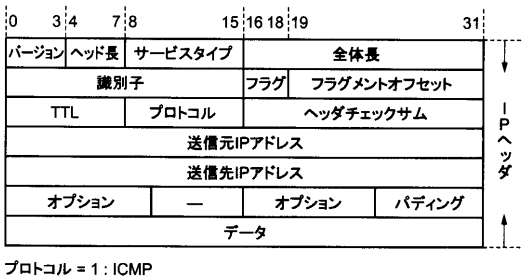
【図２】


20 ネットワーク情報検出装置
10
制御部
22
23
パケットモニタ
24
サブネットマスク
検出部
21
ネットワーク
インタフェース部
27
ネットワーク
情報設定部
25
IPアドレス
決定部
26
ルータ
検出部
28
ネットワーク
情報送信部

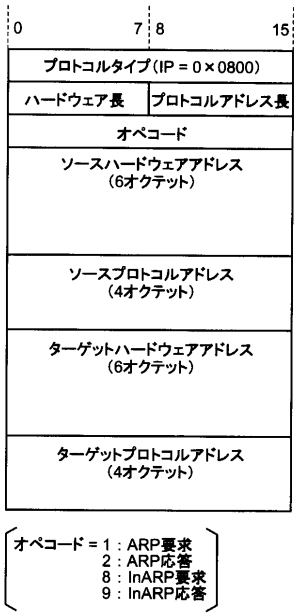
【図３】


イーサヘッダ
5
オクテット
6
オクテット
2
オクテット
最大1500
オクテット
送信先MAC
アドレス
送信元MAC
アドレス
タイプ
ユーザデータ
タイプ = 0800 : IPパケット
0806 : ARPパケット
IPパケット
ARPパケット
IPヘッダ
データ
ICMPパケット
ICMP経路変更
要求パケット
ICMPエコー要求
応答パケット
ICMP時間切れ
通知パケット

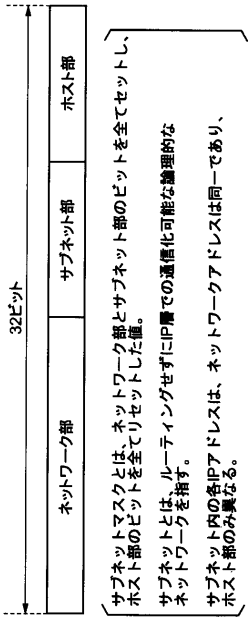
【図４】


0
3
4
7
8
15
16
18
19
31
バージョン
ヘッド長
サービスタイプ
全体長
識別子
フラグ
フラグメントオフセット
TTL
プロトコル
ヘッダチェックサム
送信元IPアドレス
送信先IPアドレス
オプション
—
オプション
パディング
データ
IPヘッダ
プロトコル = 1 : ICMP

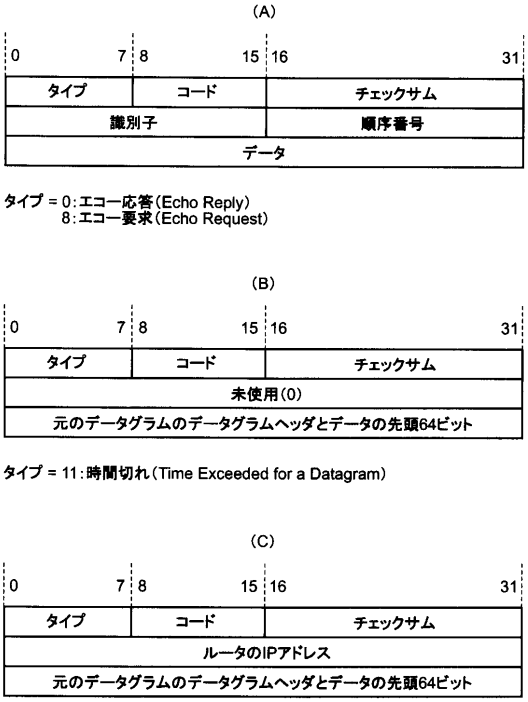
【図５】


0
7
8
15
プロトコルタイプ(IP = 0×0800)
ハードウェア長
プロトコルアドレス長
オペコード
ソースハードウェアアドレス
(6オクテット)
ソースプロトコルアドレス
(4オクテット)
ターゲットハードウェアアドレス
(6オクテット)
ターゲットプロトコルアドレス
(4オクテット)
オペコード = 1 : ARP要求
2 : ARP応答
8 : InARP要求
9 : InARP応答

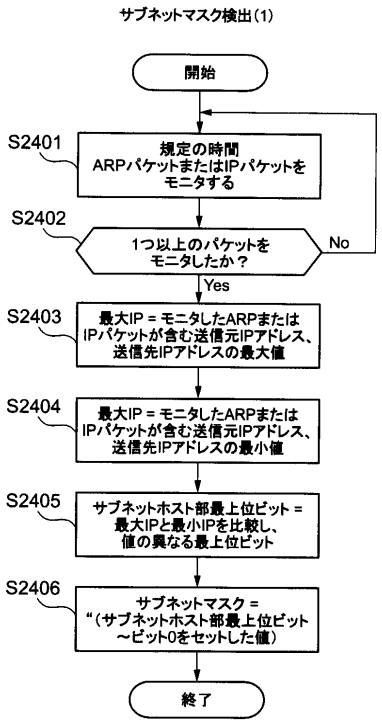
【図６】


32ビット
ネットワーク部
サブネット部
ホスト部
サブネットマスクとは、ネットワーク部とサブネット部のビットを全てセットし、ホスト部のビットを全てリセットした値。
サブネットとは、ルーティングせずにIP層での通信化可能な論理的なネットワークを指す。
サブネット内の各IPアドレスは、ネットワークアドレスは同一であり、ホスト部のみ異なる。

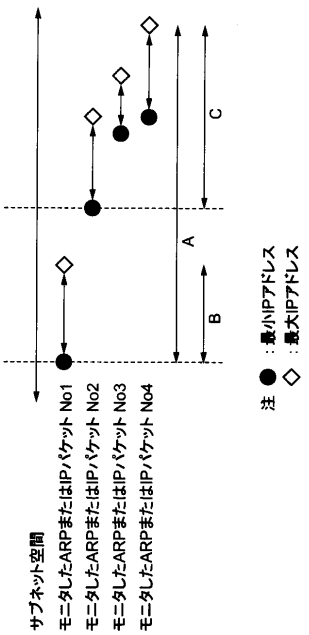
【図７】


(A)
0 7 8 15 16 31
タイプ
コード
チェックサム
識別子
順序番号
データ
タイプ = 0:エコー応答(Echo Reply)
8:エコー要求(Echo Request)
(B)
0 7 8 15 16 31
タイプ
コード
チェックサム
未使用(0)
元のデータグラムのデータグラムヘッダとデータの先頭64ビット
タイプ = 11:時間切れ(Time Exceeded for a Datagram)
(C)
0 7 8 15 16 31
タイプ
コード
チェックサム
ルータのIPアドレス
元のデータグラムのデータグラムヘッダとデータの先頭64ビット
タイプ = 5:経路変更要求(Redirect)

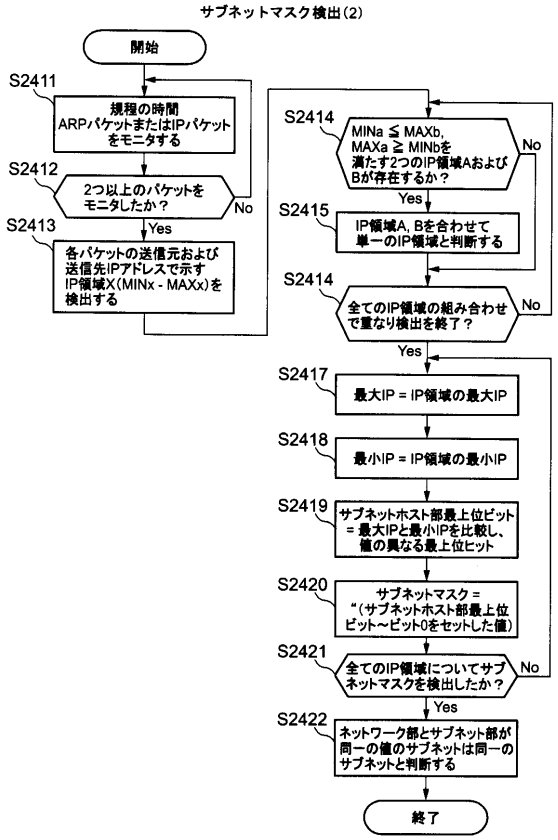
【図８】


サブネットマスク検出(1)
開始
S2401
規定の時間
ARPパケットまたはIPパケットを
モニタする
S2402
1つ以上のパケットを
モニタしたか？
No
Yes
S2403
最大IP = モニタしたARPまたは
IPパケットが含む送信元IPアドレス、
送信先IPアドレスの最大値
S2404
最小IP = モニタしたARPまたは
IPパケットが含む送信元IPアドレス、
送信先IPアドレスの最小値
S2405
サブネットホスト部最上位ビット =
最大IPと最小IPを比較し、
値の異なる最上位ビット
S2406
サブネットマスク =
“(サブネットホスト部最上位ビット
～ビット0をセットした値)
終了

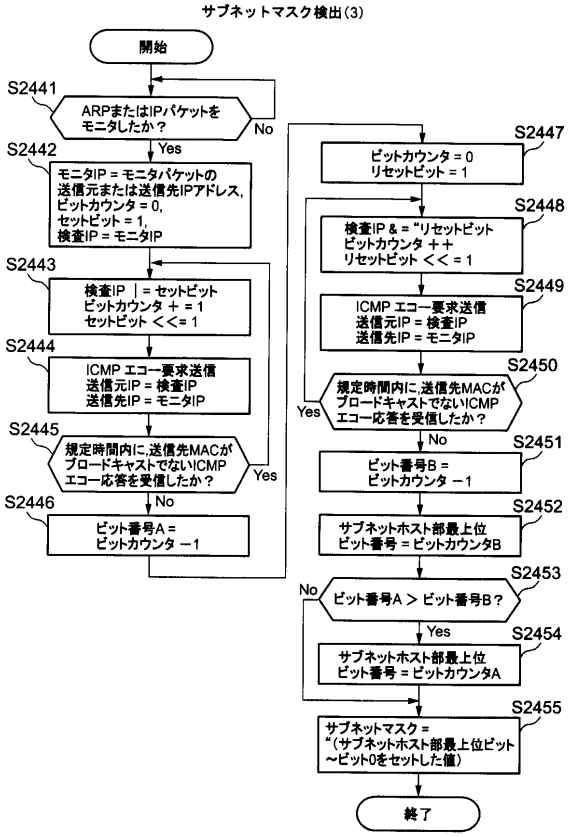
【図９】


サブネット空間
モニタしたARPまたはIPパケット No1
モニタしたARPまたはIPパケット No2
モニタしたARPまたはIPパケット No3
モニタしたARPまたはIPパケット No4
A
B
C
注 ● :最小IPアドレス
◇ :最大IPアドレス

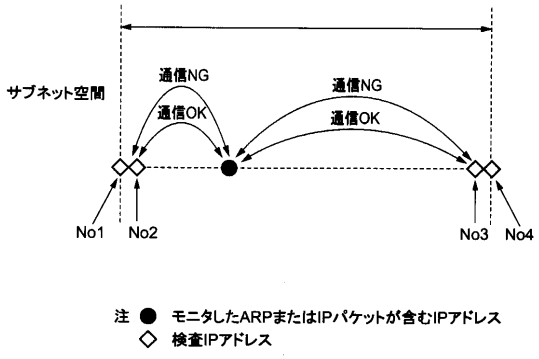
【図１０】



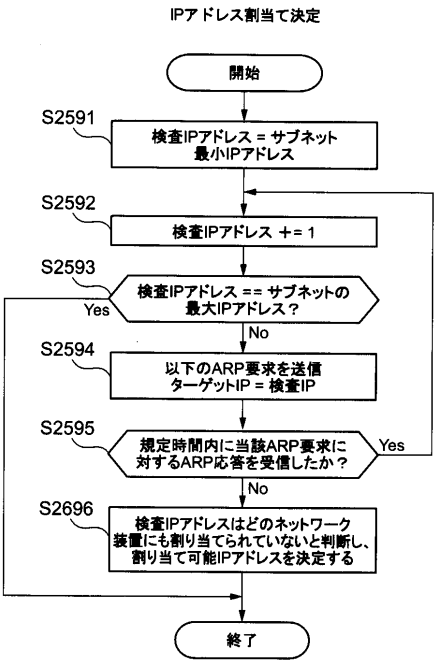
【図１１】



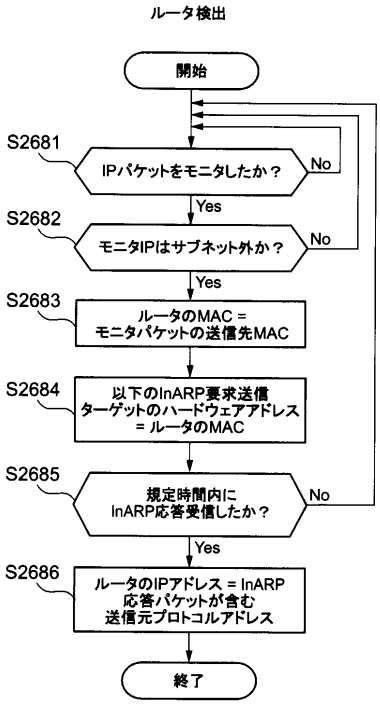
【図１２】



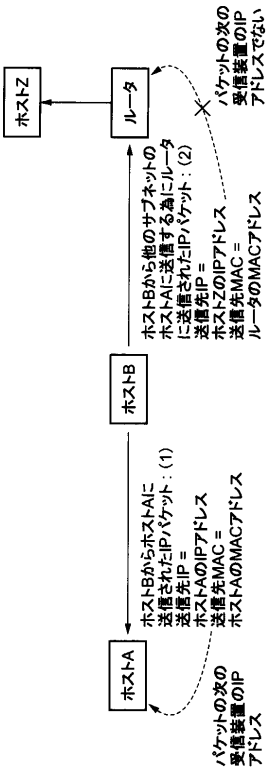
【図１３】



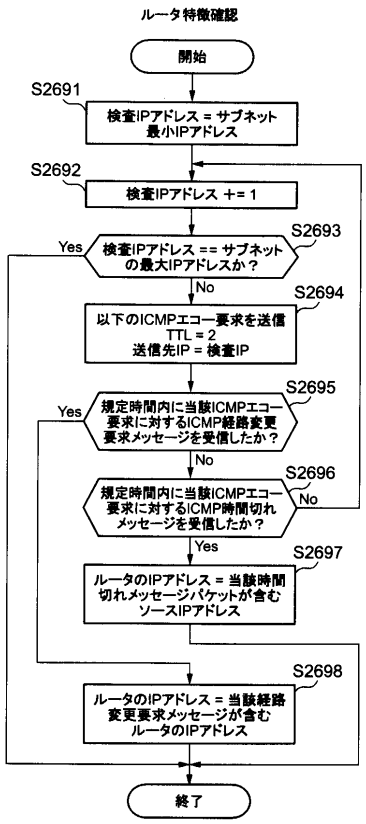
【図１４】



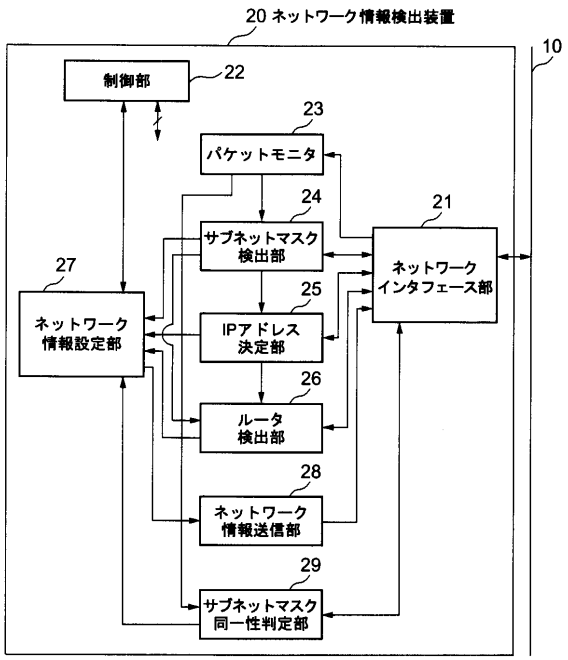
【図１５】



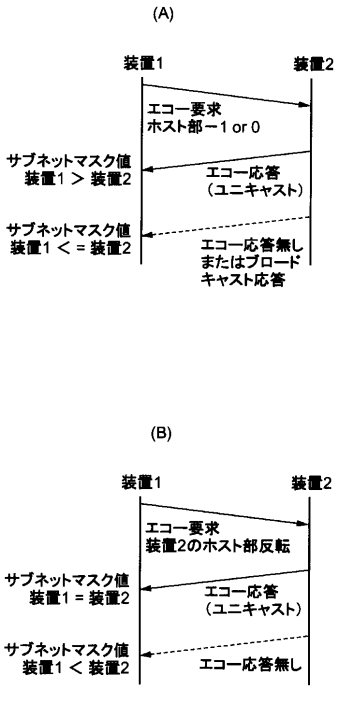
【図１６】



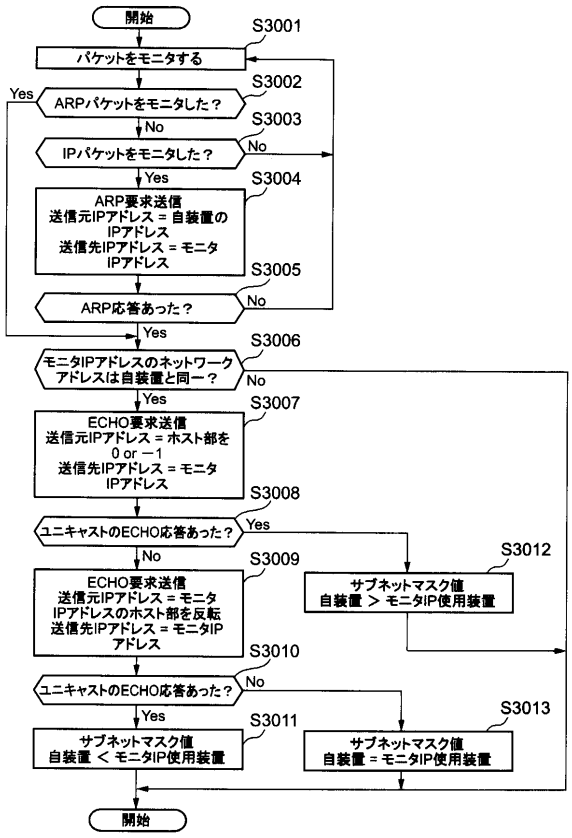
【図１７】



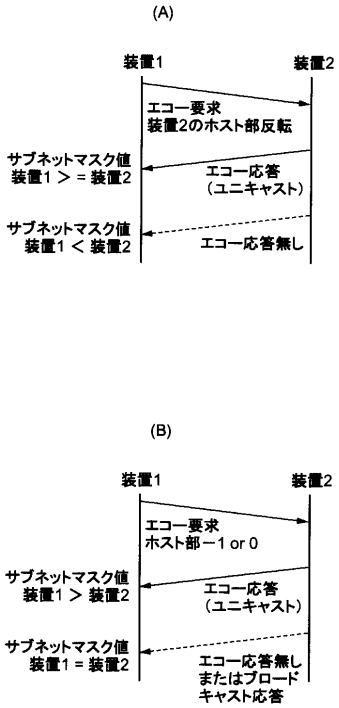
【図１８】



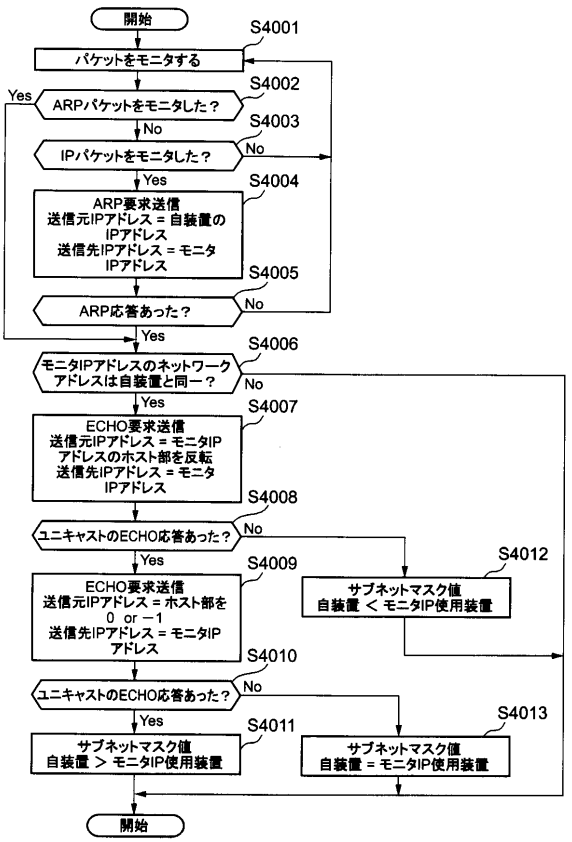
【図１９】



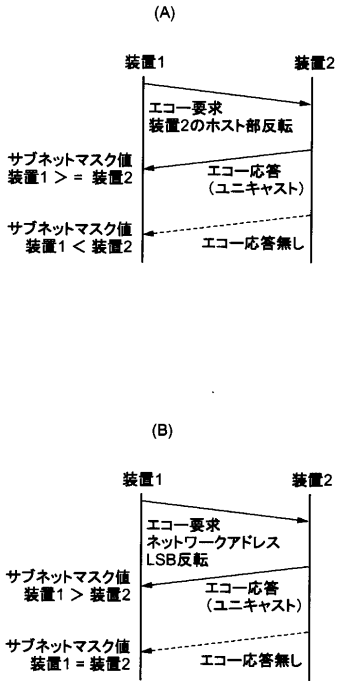
【図２０】



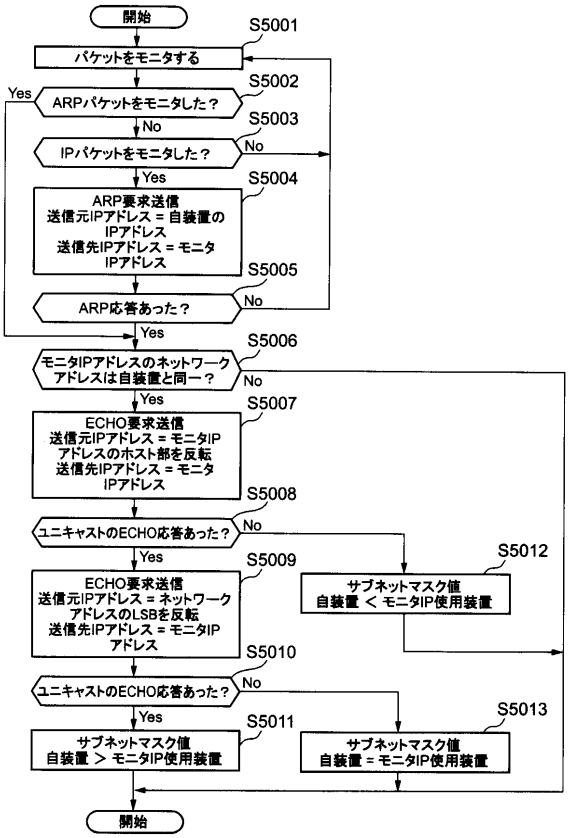
【図２１】



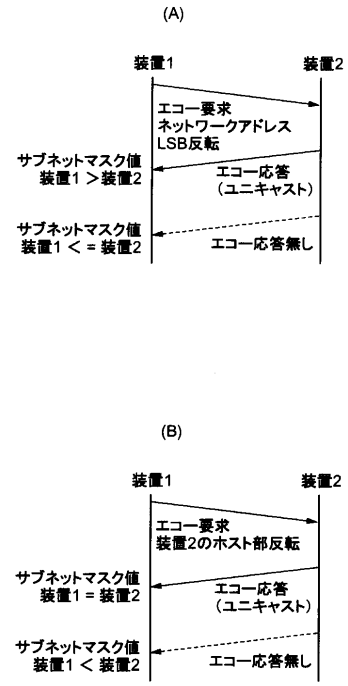
【図２２】



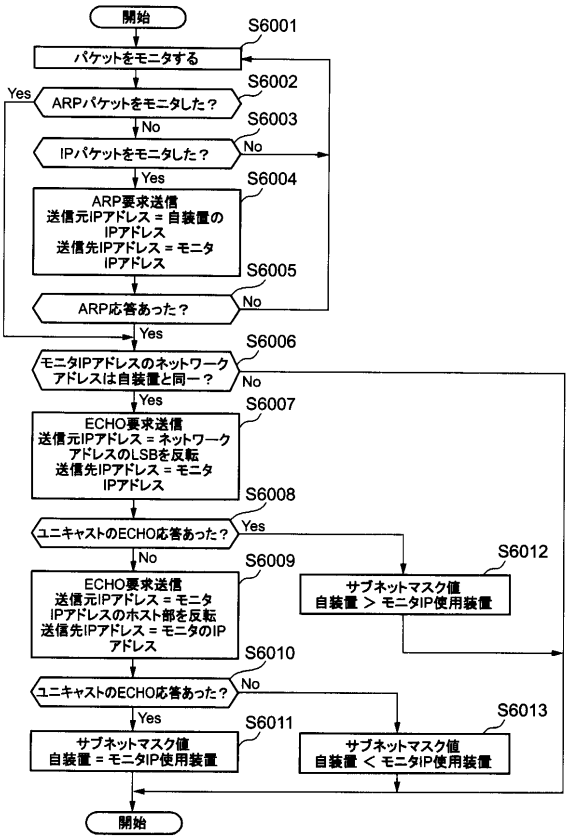
【図２３】



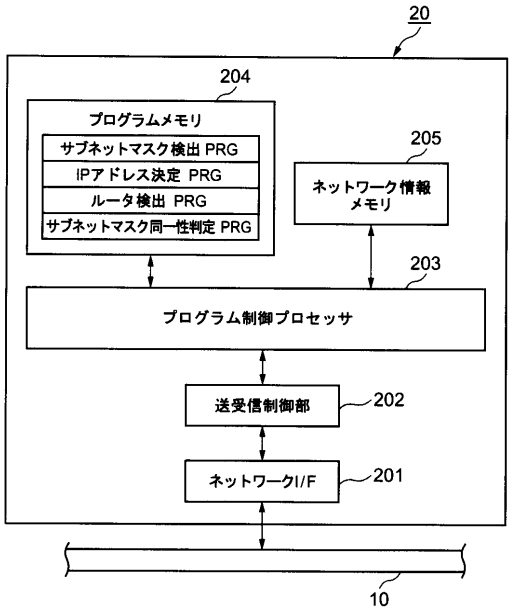
【図２４】



【図２５】



【図２６】


20
204
プログラムメモリ
サブネットマスク検出 PRG
IPアドレス決定 PRG
ルータ検出 PRG
サブネットマスク同一性判定 PRG
205
ネットワーク情報メモリ
203
プログラム制御プロセッサ
送受信制御部
202
ネットワークI/F
201
10