ルータに関するFAQ

目的

このドキュメントでは、Ciscoルータの機能や機能に関する一般的な質問に答えるとともに、その使用方法や使用方法について説明します。動画コンテンツに興味がある場合は、ここをクリックして動画の再生リストを表示してください。

該当するデバイス

- RV100シリーズ
- RV200シリーズ
- RV300シリーズ

目次

30. QoSとは何ですか。
31. RIPv1とは何ですか。RIPv2?
32. Smart Link Backupとは
33. SSL VPNとは何ですか。あなたはいつそれを使いますか？
34. VPNパススルーとは何ですか。
35. VPNとは何ですか。
36. サブネットマスク値を変更する理由は何ですか。

1.アクセスルールとは

アクセスコントロールルールは、特定のトラフィックがネットワーク上の特定のユーザとの間で送受信されることを義務付けるルールです。アクセスルールは、常に有効になるように、または定義されたスケジュールに基づいて設定できます。アクセスルールはルータまたはスイッチに設定できますが、ネットワーク内の一部またはすべてのリソースへのアクセスを許可または拒否するために、さまざまな基準に基づいて設定されます。

2. TFTPサーバのオプション66、67、および150は何ですか。

TFTPサーバを使用すると、管理者はネットワーク上のデバイスのコンフィギュレーションファイルを保存、取得、およびダウンロードできます。Dynamic Host Configuration Protocol(DHCP)サーバは、IPアドレスをネットワーク上のデバイスにリースして配布します。デバイスが起動し、IPv4またはIPv6アドレスとTFTPサーバのIPアドレスが事前に設定されていない場合、デバイスはオプション66、67、および150を使用してDHCPサーバに要求を送信します。

- DHCPオプション150はシスコ独自のプロトコルです。TFTPサーバのリストにIPアドレスが表示されます。Institute of Electrical and Electronics Engineers（IEEE；電気電子学会）の標準規格はOption 66です。
- DHCPオプション66は、単一のTFTPサーバのIPアドレスまたはホスト名を提供します。
- DHCPオプション67は、TFTPサーバのブートファイル名を提供します。

3.ルータモードとゲートウェイモードでの実行の違いは何ですか。

ルータが動作できるモードには、ルータモードとゲートウェイモードの2つがあります。ルータモードは、デバイスのネットワークアドレス変換(NAT)を無効にする動作モードで、複数のルータと複数のネットワークを接続するために使用されます。これは、ワイドエリアネットワーク環境で最も使用されます。

ルータがインターネットへのネットワーク接続をホストしている場合は、ゲートウェイモードが推奨モードです。NATは、ゲートウェイモードが有効な場合に実行されます。つまり、単一のWAN IPアドレスを使用し、LAN IPアドレスのブロック全体を持ちます。

4.システムログとは何ですか。

システムログ(Syslog)は、ネットワークイベントの記録です。システムの不具合が発生した場合は、ログを取得してシステムの問題を診断できます。ログは、ネットワークがシステムをスムーズに実行し、障害を防止する方法を理解するために使用される重要なツールです。ネットワーク管理、トラブルシューティング、およびモニタリングに役立ちます。

5. DHCPモードとは何ですか。

Dynamic Host Configuration Protocol(DHCP)には、次の2つのモードがあります。DHCPサーバと

DHCPリレー。DHCPサーバは、ネットワーク上のDHCPクライアントまたはホストに使用可能なIPアドレスを自動的に割り当てます。DHCPサーバとDHCPクライアントは、同じネットワークリンクに接続されている必要があります。クライアントとサーバが同じ物理サブネット上にない大規模なネットワークでは、各ネットワークリンクに1つ以上のDHCPリレーエージェントが含まれています。DHCPリレーエージェントはルータになることができます。クライアントがルータにDHCP要求を送信すると、ルータはクライアントのIPアドレスを指定するように要求して、その要求をDHCPサーバに転送します。DHCPサーバはルータに応答を送信し、ルータはその応答をクライアントに転送します。ルータとDHCPサーバは、機能するために同じサブネット上にある必要はありません。ルータは、クライアントとDHCPサーバ間の連絡窓口として機能します。

6. 3G/4Gとは何ですか。

モバイルブロードバンドまたはワイヤレスインターネット用のテクノロジーで、携帯電話またはポータブルモデムを介してアクセスできます。文字Gは世代を表します。4Gテクノロジーは、Long Term Evolution(LTE)に次ぐ最新かつ最速の1つです。 一部のCisco VPNルータでは、サポートされている3G/4G USBドングルからインターネット接続を共有できます。このドングルは、メインのインターネットサービスプロバイダー(ISP)がダウンまたはダウンした場合にフェールオーバーとして機能します。

7.証明書ジェネレータとは何ですか。また、いつ使用しますか。

デジタル証明書は、証明書の名前付きサブジェクトによって公開キーの所有権を証明します。これにより、証明書利用者は、認証された公開キーに対応する秘密キーによる署名やアサーションに依存できます。ルータは、自己署名証明書、つまりネットワーク管理者によって作成された証明書を生成できます。また、認証局(CA)に要求を送信して、デジタルID証明書を申請することもできます。サードパーティアプリケーションから正当な証明書を取得することが重要です。

8.ファイアウォールとは何ですか。また、いつ使用しますか。

ファイアウォールの主な目的は、データパケットを分析し、事前に決められたルールセットに基づいて通過を許可するかどうかを決定することによって、着信および発信ネットワークトラフィックを制御することです。ルータは、着信データのフィルタリングを可能にする機能により、強力なハードウェアファイアウォールと見なされます。ネットワークファイアウォールは、セキュアで信頼できると想定される内部ネットワークと、セキュアで信頼できないと想定されるインターネットなどの外部インターネットワークとの間にブリッジを構築します。

9.信頼できるIPSec証明書とは何ですか。

Internet Protocol Security(IPSec)は、IPネットワーク上でセキュアで認証され、信頼性の高い通信を生成します。これは、Secure Socket Layer(SSL)証明書を使用したオンライントランザクションのセキュア認証および検証のキー生成および認証データ、キー確立プロトコル、暗号化アルゴリズム、または認証メカニズムの交換に使用されます。RV320では、自己署名またはサードパーティCAによって承認された最大50の証明書を追加できます。これらの証明書は、コンピュータまたはUSBデバイスにエクスポートし、クライアントまたは管理者が使用するようにインポートできます。

10.信頼できるSSL証明書とは何ですか。

証明書は、コンピュータまたはインターネット上のユーザIDを確認し、プライベートまたはセキュアな会話を強化するために使用されます。Secure Sockets Layer(SSL)は、Webサーバとブラウザの間に暗号化されたリンクを作成するための標準のセキュリティテクノロジーです。これらの証明書は、コンピュータまたはUSBデバイスにエクスポートし、クライアントまたは管理者が使

用するようにインポートできます。

11.クライアントからゲートウェイへのVPNとは何ですか。

Client-to-Gateway Virtual Private Network(VPN)とは、地理的に異なる場所にある会社の別のブランチにリモート接続して、データをより安全に送受信できることを意味します。通常、Cisco AnyConnect Secure Mobility ClientなどのVPNクライアントソフトウェアがコンピュータにインストールされ、ログインします。

注：バージョン1.0.3.15以降、RV340シリーズのライセンス要件に関する更新が行われています。詳細については、ここをクリックしてください。

12.コンテンツフィルタリングとは何ですか。

コンテンツフィルタリングは、管理者が指定された不要なWebサイトをブロックできるようにする機能です。コンテンツフィルタリングでは、キーワードやUniform Resource Locator(URL)に従って、リストをブロックし、Webサイトへのアクセスを許可できます。 管理者は、アクティブにするタイミングに応じて、コンテンツフィルタリングにスケジュールを適用できます。

詳細については、用語集を参照してください。

13. CoSとは

Class of Service（CoS；サービスクラス）は、他の種類のトラフィックよりもプライオリティを割り当てて、ネットワーク上のトラフィックを管理する方法です。これは、ネットワークトラフィックのイーサネットフレームヘッダーにプライオリティレベルを割り当てるために使用され、トランクリンクにのみ適用されます。トラフィックを区別することで、ネットワークで輻輳や遅延などの問題が発生した場合に、優先データパケットをポリシングして送信の優先順位を付けることができます。CoSプライオリティ設定をルータのトラフィック転送キューにマッピングできます。

14. DHCPオプション82とは何ですか。

DHCPリレーは、ホストと同じネットワーク上にないリモートDHCPサーバ間のDHCP通信を可能にするルータに含まれる機能です。オプション82は、DHCPリレーエージェント情報オプションで、クライアントから発信されたDHCPパケットをDHCPサーバに転送するときに、DHCPリレーエージェントが自身に関する情報を含めることができます。DHCPサーバはこの情報を使用して、IPアドレッシングまたはその他のパラメータ割り当てポリシーを実装できます。接続を完全に識別することにより、DHCPプロセスにセキュリティが追加されます。

15. DHCPとは何ですか。

Dynamic Host Configuration Protocol(DHCP)は、ネットワーク上のデバイスのIPアドレスを自動的に設定するネットワークコンフィギュレーションプロトコルで、デバイスにIPアドレスを手動で割り当てるのではなく、相互に接続できます。

16. DMZとは何ですか。また、いつ使用すればよいですか。

Demilitarized Zone（DMZ；非武装地帯）は、ファイアウォールの背後で公開されているサブネットワークです。DMZを使用すると、WANポートに着信するパケットをLAN内の特定のIPアドレスにリダイレクトできます。LANまたはWANの両方からDMZ内の特定のサービスおよびポートへのアクセスを許可するようにファイアウォールルールを設定できます。DMZノードに対する攻撃の場合、LANは必ずしも脆弱ではありません。WANに公開する必要があるホスト（Webサーバや電

子メールサーバなど）をDMZネットワークに配置することを推奨します。

17. DSCPとは何ですか。

Differentiated Services Code Point(DSCP)は、ネットワークトラフィックを分類し、IPヘッダーフィールドでDSCPコードでマーキングすることによって、パケットにさまざまなレベルのサービスを割り当てるために使用されます。DSCP設定は、DSCP値がQuality of Service(QoS)にどのようにマッピングされるかを指定します。これは、ネットワーク上のトラフィックのプライオリティレベルを管理する方法です。ルータがType of Service(ToS)オクテットのプライオリティビットを使用して、レイヤ3のトラフィックにQoSよりも優先できるのは、DSCPです。

18.ダイナミックDNSとは何ですか。

Dynamic Domain Name System（DNS；ダイナミックドメインネームシステム）は、DNS内のネームサーバを自動的に更新する方法で、多くの場合、リアルタイムで、設定されたホスト名、アドレス、またはその他の情報のアクティブなDDNS設定を使用します。このサービスは固定ドメイン名をダイナミックWAN IPアドレスに割り当てるため、LAN上で独自のWeb、FTP、または別のタイプのTCP/IPサーバをホストできます。ルータは、WebベースのDDNSアカウントを介してDDNSを使用します。ルータのWAN IPアドレスが変更されると、DDNS機能は変更をDDNSサーバに通知します。DDNSサーバは、新しいWAN IPアドレスを含むように設定を更新します。これは、ルータのWAN IPアドレスが頻繁に変更される場合に便利です。ルータのDDNS機能を使用するには、提供されているWebサイトのいずれかにDDNSアカウントを作成する必要があります。

19.ゲートウェイ間VPNとは何ですか。あなたはいつそれを使いますか？

ゲートウェイ間VPN接続では、2台のルータが互いにセキュアに接続し、一方の端のクライアントが、もう一方の端のネットワークの一部であるかのように論理的に表示できます。これにより、データとリソースをインターネット経由でより簡単かつ安全に共有できます。ゲートウェイ間VPNを有効にするには、両方のルータで設定を行う必要があります。

20. IPおよびMACバインディングとは何ですか。いつ使えばいい？

IPアドレスとMACアドレスのバインディングは、IPアドレスをMACアドレスに、またはその逆にリンクするプロセスです。ルータが同じIPアドレスで異なるMACアドレスのパケットを受信すると、そのパケットは廃棄されます。IPスプーフィングを防止し、デバイスのIPアドレスを変更できないため、ネットワークセキュリティを強化します。トラフィックの送信元ホストのIPアドレスとMACアドレスは、常に一致してネットワークへのアクセスを許可する必要があります。ルータが同じIPアドレスで異なるMACアドレスのパケットを受信すると、そのパケットは廃棄されます。

21.ロードバランシングとは何ですか。また、いつ使用しますか。

ロードバランシングにより、ルータは特定の宛先への複数のベストパスを利用できます。これはルータでの転送プロセス固有の機能で、ルーティング テーブルに宛先への複数のパスがある場合に自動的に起動されます。ルータでロードバランシングを設定すると、リソースの適切な使用率を実現し、スループットと応答時間を最大化し、複数のコンピュータ、ネットワークリンク、その他のさまざまなリソースにワークロードを分散するため、負荷の増大を回避できます。

22. MACアドレスクローンとは何ですか。また、いつ使用する必要がありますか。

MACアドレスクローンは、あるデバイスのMACアドレスの正確なコピーを、ルータなどの別のデバイスに複製する最も簡単な方法です。場合によっては、ISPからルータのMACアドレスを登録

してデバイスを認証するように求められることがあります。MACアドレスは、ハードウェアごとに12桁の16進数コードで、一意に識別できます。すでにISPに別のMACアドレスを登録している場合は、MACアドレスクローンを使用して、そのアドレスを新しいルータに複製できます。この方法では、以前に登録したMACアドレスを変更するためにISPに連絡する必要がないため、メンテナンスのコストと時間を削減できます。

23. 1対1 NATとは何ですか。また、いつ使用する必要がありますか。

1対1のネットワークアドレス変換(NAT)は、有効なWAN IPアドレスを、NATによってWAN（インターネット）から隠されているLAN IPアドレスにマッピングする関係を作成します。これにより、LANデバイスが検出および攻撃から保護されます。ルータでは、単一のプライベートIPアドレス（LAN IPアドレス）を単一のパブリックIPアドレス（WAN IPアドレス）にマッピングするか、またはプライベートIPアドレスの範囲をパブリックIPアドレスの範囲にマッピングできます。

24.パスワードの複雑さとは何ですか。また、なぜ私にとって有益なのですか。

パスワードの複雑度は、パスワードの変更に関する最小限のパスワードの複雑度を適用するネットワークデバイスの機能です。これは、すべてのタイプのネットワークに有益です。複雑なパスワードは、指定した時間が経過すると期限切れになるように設定できます。

25.ポートアドレス変換(PAT)とは何ですか。また、いつ使用する必要がありますか。

これは、プライベートネットワークまたはローカルネットワーク内の複数のデバイスを1つのパブリックIPアドレスにマッピングできる機能です。PATは、IPアドレスを節約するために使用されます。ネットワークアドレス変換(NAT)の拡張です。PATは、ポーティング、ポートオーバーロード、ポートレベル多重化NAT、シングルアドレスNATとも呼ばれます。

26.ポート転送とは何ですか。また、いつ使用する必要がありますか。

ポート転送は、プライベートLAN内の特定のデバイスにデータを渡すために使用される機能です。これは、デバイス上の選択されたポートからネットワーク上の対応するポートにトラフィックをマッピングすることによって行われます。ルータはこの機能をサポートしているため、パフォーマンスとネットワークバランシングの特性を改善するために、必要な場所にトラフィックを効率的に転送できます。ポート転送は、設定されたポートが常に開いているため、セキュリティ上のリスクがあるため、必要な場合にのみ使用してください。

27.ポートミラーリングとは

ポートミラーリングは、ネットワークトラフィックを監視するために使用される方法です。ポートミラーリングを使用すると、ネットワークデバイスのポート（送信元ポート）での着信パケットと発信パケットのコピーが、パケットが調べられるほかのポート（ターゲットポート）に転送されます。

28.ポートトリガーとは何ですか。また、いつ使用する必要がありますか。

ポートトリガーはポート転送に似ていますが、着信ポートが常に開いていないため、より安全です。ポートはトリガーされるまで閉じられたままで、不要なポートアクセスの可能性を制限します。ポートトリガーは、ダイナミックポートフォワーディングの方式です。ルータに接続されているホストが、ポート範囲トリガールールで設定されているトリガーポートを開くと、ルータは設定されたポートをホストに転送します。ホストがトリガーポートを閉じると、ルータは転送ポ

ートを閉じます。ネットワーク上のコンピュータは、ポートフォワーディングとは異なり、着信ポートの転送に内部IPアドレスを必要としないため、ポートトリガーセットアップを使用できます。

29. PPTPサーバとは何ですか。あなたはいつそれを使いますか？どのように設定しますか。

Point-to-Point Tunneling Protocol(PPTP)は、パブリックネットワーク間にVPNトンネルを実装するために使用されるネットワークプロトコルです。PPTPサーバは、Virtual Private Dialup Network(VPDN)サーバとも呼ばれます。 PPTPは、Transmission Control Protocol（TCP；伝送制御プロトコル）上の制御チャネルと、PPPパケットをカプセル化するために動作するGeneric Routing Encapsulation（GRE；総称ルーティングカプセル化）トンネルを使用します。PPTPクライアントソフトウェアを実行しているユーザには、最大25のPPTP VPNトンネルを有効にできます。最も一般的なPPTPの実装は、Microsoft Windows製品ファミリで行われ、Windows PPTPスタックの標準機能として、異なるレベルの認証と暗号化をネイティブに実装します。PPTPは高速で、モバイルデバイスで動作できるため、他のプロトコルよりも優先されます。参考として、ここをクリックして、設定方法を確認してください。

30. QoSとは何ですか。

Quality of Service(QoS)は、主にネットワークのパフォーマンスを向上させるために使用され、ユーザに必要なサービスを提供するために使用されます。トラフィックのタイプに基づいてトラフィックフローの優先順位を設定します。QoSは、遅延の影響を受けやすいアプリケーション（音声やビデオなど）の優先順位付けされたトラフィックに適用でき、遅延の影響を受けないトラフィック（バルクデータ転送など）の影響を制御できます。

31. RIPv1とは何ですか。RIPv2?

Routing Information Protocol(RIP)は、ルータがルーティング情報を交換するために使用するディスタンスベクタープロトコルです。RIPは、ルーティングメトリックとしてホップカウントを使用します。RIPは、送信元から宛先までのパスで許可されるホップ数の制限を実装することによって、ルーティングループが無期限に継続することを防止します。RIPの最大ホップカウントは15で、サポートできるネットワークサイズを制限します。これが、RIPv2が開発された理由です。クラスフルRIPv1とは異なり、RIPv2は、ルーティングアップデートを送信するときにサブネットマスクを含むクラスレスルーティングプロトコルです。

RIPv2でルートを集約することで、大規模ネットワークの拡張性と効率が向上します。IPアドレスの集約は、RIPルーティングテーブルに子ルート（集約アドレスに含まれる個々のIPアドレスの任意の組み合わせに対して作成されたルート）のエントリがないことを意味し、テーブルのサイズを縮小し、ルータがより多くのルートをく処理できます。

32. Smart Link Backupとは何ですか。

Smart Link Backupは、ユーザが最初のWANまたはプライマリリンクに障害が発生した場合に2番目のWANを設定できるようにする機能です。この機能は、WANとデバイス間の通信が常に継続することを保証するために使用されます。この機能は、デュアルWAN接続を持つルータにあります。

33. SSL VPNとは何ですか。あなたはいつそれを使いますか？

Secure Sockets Layer Virtual Private Network(SSL VPN)は、WebVPNとも呼ばれ、最新のWebブラウザに組み込まれたSSL機能を使用してリモートアクセスVPN機能を提供するテクノロジーで

す。これは、クライアントのデバイスにVPNクライアントをインストールする必要はありません。SSL VPNを使用すると、インターネット対応の任意の場所のユーザがWebブラウザを起動してリモートアクセスVPN接続を確立できるため、生産性の向上と可用性の向上、VPNクライアントソフトウェアとサポートのITコストの削減が可能になります。

34. VPNパススルーとは何ですか。

VPNパススルーは、インターネット上で2つのセキュアなネットワークを接続する方法です。これは、ルータに接続されたVPNクライアントから生成されたVPNトラフィックがインターネットに通過できるようにし、VPN接続が成功するようにするために使用されます。

35. VPNとは何ですか。

バーチャルプライベートネットワーク(VPN)は、トンネルを作成することによってネットワーク内またはネットワーク間に確立されるセキュアな接続です。VPNは、指定されたホストとネットワーク間のトラフィックを、許可されていないホストとネットワークのトラフィックから分離するのに役立ちます。VPNは、拡張性が高く、ネットワークトポロジを簡素化し、リモートユーザの出張時間とコストを削減することで生産性を向上させる方法で、企業にとって有益です。

36.サブネットマスク値を変更する理由は何ですか。

サブネットは、特定のサブネットアドレスを共有するネットワークの一部です。サブネットマスクは、ネットワークアドレスのどの部分がサブネットを参照し、どの部分がホストを参照するかを表すために使用される32ビットの組み合わせです。ホストがネットワークと通信できない場合は、サブネットマスクの値を変更できます。管理者が物理的な変更を行わずにサブネットワーク上のホスト数を増やしたい場合は、サブネットマスクも変更できます。