

Unidade III

5 OS PROTOCOLOS ICMP, ARP E DOMÍNIOS DE COLISÃO

5.1 ICMP — Internet Control Message Protocol

ICMP é um protocolo que, conjuntamente com o IP, opera na camada 3 do modelo OSI. Entretanto, não é usado especificamente para transmissão dos dados, mas sim como protocolo de controle que auxilia o bom funcionamento do protocolo IP.

Ao executar um **ping** ou um **traceroute** em roteadores ou computadores, estamos usando o ICMP.

A funcionalidade efetiva do ICMP permite que equipamentos roteadores e ativos de rede interligados possam informar erros ou quaisquer problemas inesperados ocorridos durante uma transmissão de dados.

O ICMP é um mecanismo que informa os erros e possibilita que roteadores possam avisar às entidades transmissoras as causas de um erro. Entretanto, o ICMP não especifica totalmente a ação que precisa ser realizada para a correção de um erro.

Vamos imaginar que, durante uma transmissão, um pacote passa por vários roteadores até o seu destino. Caso o destinatário receba informações erradas sobre o roteamento, esse pacote será encaminhado para um roteador errado. Logo, esse que recebeu os dados não tem condições de enviar informações de erro ao destinatário original, porém ele consegue avisar ao transmissor original do pacote esta anomalia ocorrida. Dessa maneira, concluímos que o transmissor não tem qualquer influência sobre os problemas de roteamento que possam vir a acontecer durante o trajeto do pacote e também não tem condições de identificar em qual roteador aconteceu o problema.

Na tabela a seguir, vemos os tipos de mensagem que são enviadas pelo protocolo ICMP.

Tabela 10 – Tabela de mensagens de erro do protocolo ICMP

Tipo	Código	Descrição
0	0	echoreply
		destination unreachable
	0	network unreachable
	1	host unreachable
	2	protocol unreachable
	3	port unreachable

	4	fragmentation needed but don't fragmentation bit set
	5	source route failed
	6	destination network unknown
3	7	destination host unknown
	8	source host isolated (obsolete)
	9	destination network administratively prohibited
	10	destination host administratively prohibited
	11	network unreachable for TOS
	12	host unreachable for TOS
	13	communication administratively prohibited filtering
	14	host precedence violation
	15	precedence cutoff in effect
4	0	source quench (controle de fluxos)
		Redirect
	0	redirect for network
5	1	redirect for host
	2	redirect for type-of-service and network
	3	redirect for type-of-service and host
8	0	echo request
9	0	router advertisement
10	0	router solicitation
		time exceeded
11	0	time-to-live equals 0 during transit
	1	time-to-live equals 0 during reassembly
		parameter problem
12	0	ip reader bad
	1	required option missing
13	0	Timestamprequest
14	0	Timestampreply
15	0	Informationrequest
16	0	Informationreply
17	0	address mask request
18	0	address mask reply

5.2 A comparação entre o ICMPv4 e ICMPv6

Existe um consenso entre os autores e administradores de rede sobre a confiabilidade do protocolo IP. A suíte dos protocolos TCP/IP tem a previsão do envio de mensagens no caso de determinados erros, essas mensagens são encaminhadas com o serviço e ICMP. A razão dessas mensagens é dar uma resposta sobre as questões relativas ao processamento dos pacotes IP, baseado em certas condições, e não exatamente tornar o IP mais confiável. As mensagens ICMP não são necessárias muitas das vezes, também não são permitidas, por questões de segurança, em todas as vezes.

O protocolo ICMP está disponível tanto para versão IPv4 como para versão IPv6. O ICMPv4 é um protocolo de mensagens específicas para o IPv4, já o ICMPv6 oferece os mesmos serviços, porém para o protocolo IPv6, mas este ainda inclui funcionalidades adicionais importantes na análise de tráfego.

Algumas das mensagens ICMP mais comuns, tanto para ICMPv4 e ICMPv6, são:

- Confirmação de host.
- Destino ou serviço inalcançável.
- Tempo excedido.
- Redirecionamento de rota.

5.2.1 Confirmação de host

Uma mensagem proveniente do eco ICMP pode ser usada para determinar se o host está ou não operacional. O host local envia uma solicitação de eco no padrão ICMP (ECHO REQUEST) para um host, se o host estiver ativo e disponível, o host de destino enviará uma resposta de eco (ECHO REPLY).

5.2.2 Destino ou serviço inalcançável

No momento que o host ou gateway recebe um pacote e este não pode ser entregue, ele pode fazer uso de uma mensagem ICMP de destino inalcançável para notificar à origem do datagrama que o destino ou serviço está inalcançável. Essa mensagem conterá um código que indica o motivo pelo qual não foi possível entregar o pacote.

Alguns dos códigos de destino inalcançável para ICMPv4 são:

- 0 = rede inalcançável.
- 1 = host inalcançável.
- 2 = protocolo inalcançável.
- 3 = porta inalcançável.



Observação

Observação importante é que o ICMPv6 tem códigos semelhantes em relação ao ICMPv4, mas com certas diferenças para mensagens de destino inalcançável.

5.2.3 Tempo excedido

Uma mensagem ICMPv4 de tempo excedido é usada por um roteador para indicar que um determinado pacote não pode ser encaminhado porque seu tempo de vida útil TTL (time to live) foi reduzido a zero. Caso o roteador receba um novo pacote, o campo TTL (time to live) do pacote IPv4 diminui para zero, ele então descartará o pacote e enviará uma mensagem de tempo excedido para o host da origem.

No caso do ICMPv6, este roteador enviará uma mensagem de tempo excedido, caso o roteador não esteja conseguindo encaminhar um pacote IPv6, basicamente porque o pacote expirou. O IPv6 não tem um campo TTL (time to live) ativo, em vez disso, ele usa um campo referente ao limite de saltos para determinar se o pacote expirou ou não.

5.2.4 Mensagens ICMPv6: solicitação de roteador e anúncio de roteador

As mensagens informacionais de erro encontradas nos ICMPv6 são muito parecidas com as mensagens de controle de erro que foram implementadas no ICMPv4. Entretanto, o ICMPv6 tem aprimoramentos em suas funções e novos recursos que não são encontrados nos ICMPv4. As mensagens ICMPv6 são encapsuladas diretamente pelo datagrama IPv6.

O ICMPv6 inclui quatro novos protocolos como parte do protocolo ND ou NDP (Neighbor Discovery Protocol):

- Mensagens entre um roteador IPv6 e um dispositivo IPv6:
 - Mensagem de Solicitação de Roteador (RS);
 - Mensagem de Anúncio de Roteador (RA).
- Mensagens entre dispositivos IPv6:
 - Mensagem de Solicitação de Vizinho (NS);
 - Mensagem de Anúncio de Vizinho (NA).

A figura a seguir mostra um bom exemplo de um PC e de um roteador trocando mensagens de solicitação de anúncio de roteador.

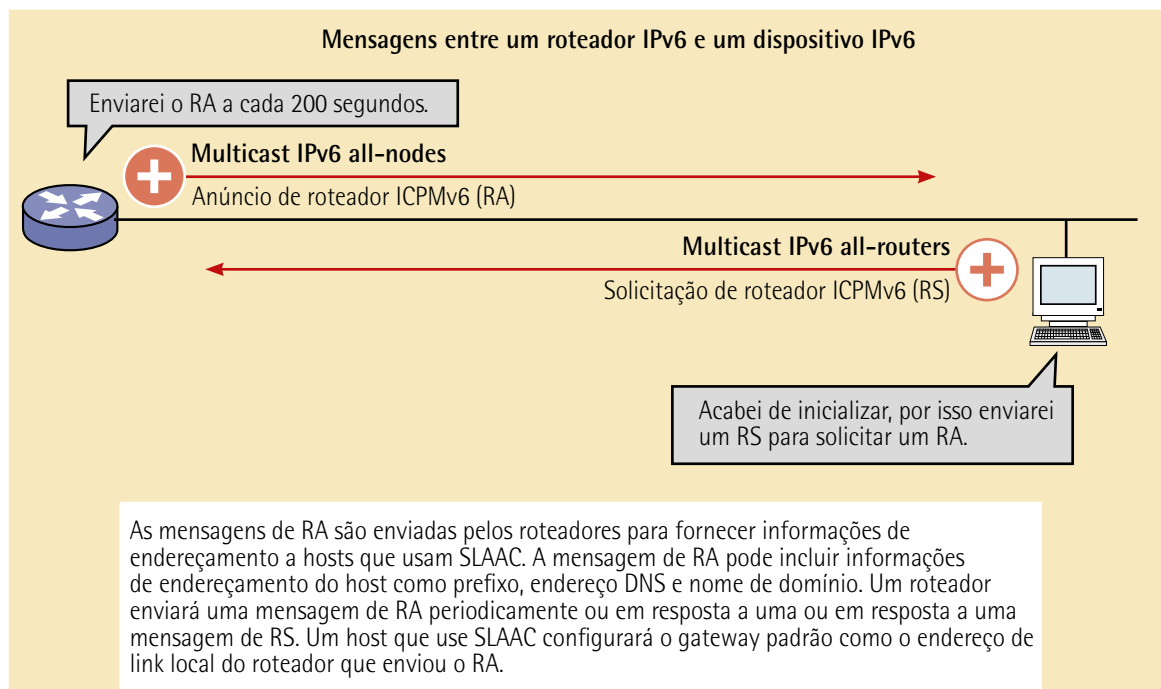


Figura 69 – Mensagem do roteador R1 para dispositivo de usuário formato IPv6

As mensagens de solicitação e de anúncio de vizinho são usadas para resolução e detecção de endereços duplicados (DAD).

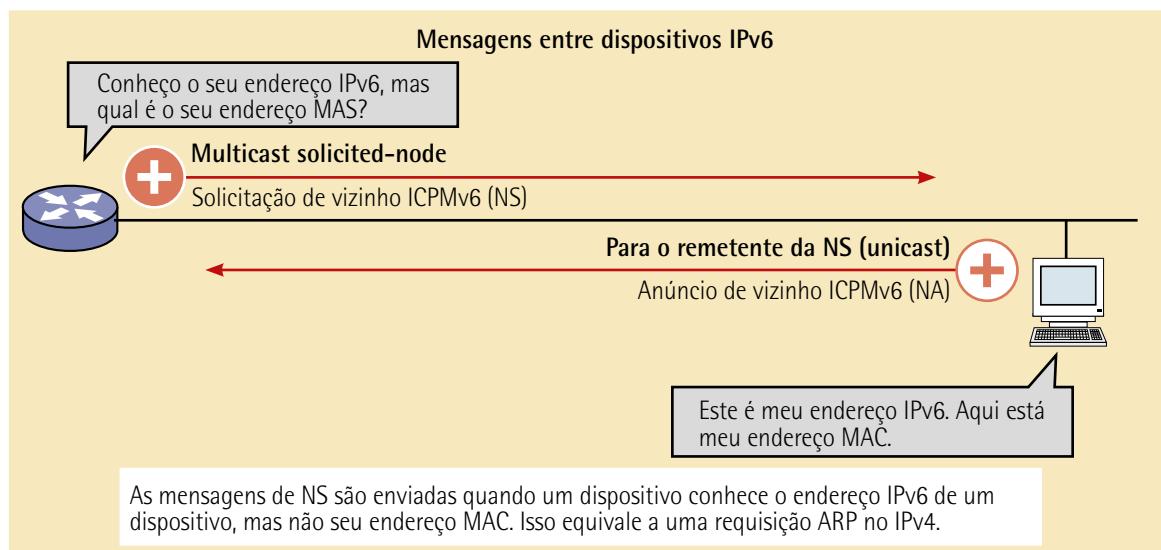


Figura 70 – Mensagem entre dispositivos do protocolo IPv6

5.2.5 Resolução de endereços

A resolução de endereço IPv6 é usada quando um dispositivo na LAN sabe o endereço IPv6 unicast de um destino, mas não conhece seu MAC Ethernet. A fim de detectar o endereço MAC destino ou dispositivo final, este enviará uma mensagem NS para o endereço do nó solicitado. Esta mensagem carregará consigo o endereço IPv6 do destino conhecido, o destino alvo dentro do barramento IPv6 responderá com uma mensagem NA contendo o seu MAC Ethernet.

5.2.6 Detecção de endereços duplicados (DAD)

No momento em que um dispositivo recebe uma chamada unicast global ou o endereço unicast de link local, a recomendação é executar o DAD de endereço para garantir que ele seja absolutamente único no barramento. A verificação de exclusividade de endereço força esse dispositivo a enviar uma mensagem NS com seu próprio endereço IPv6 como endereço IPv6 de destino, se outro dispositivo dentro da rede tiver o mesmo endereço, ele responderá com a mensagem NA. Essa mensagem de NA promoverá uma notificação ao dispositivo emissor de que esse endereço já está em uso.

Se qualquer mensagem de NA correspondente não for devolvida em um determinado período de tempo, o endereço unicast será único e aceitável para uso.

Observação

Embora a DAD não seja obrigatória, a RFC 4861 recomenda que ela seja executada em endereços unicast.

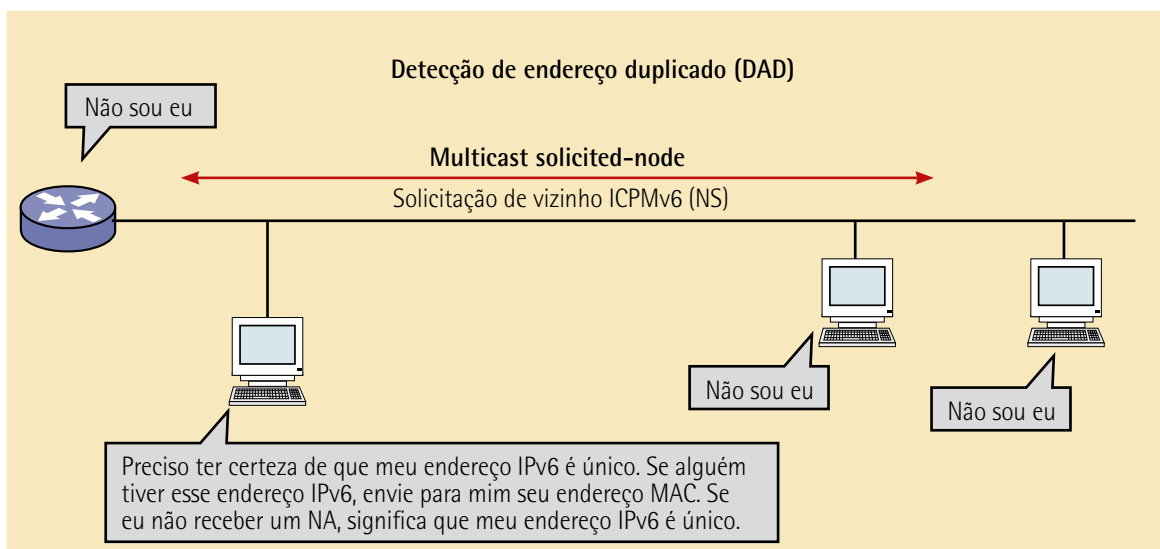


Figura 71 – Mensagem do serviço DAD do protocolo IPv6

5.2.7 Ping: teste da pilha local

O ping é o utilitário de teste que utiliza o protocolo ICMP, além de suas mensagens de solicitação de eco e de uma resposta de eco, para aferir a conectividade entre dois hosts. O ping tem funcionalidade garantida com hosts IPv4 e hosts IPv6.

Para aferir a conectividade com outro host em uma rede, uma solicitação de eco é enviada ao host usando um comando ping. Se fosse o endereço específico a receber tal requisição de eco, este enviará uma resposta de eco equivalente. À medida que a resposta de eco é recebida, o ping nos fornece uma resposta sobre o tempo de envio da requisição e o recebimento da resposta, esta pode ser uma medida de desempenho da rede. Basicamente, ela é referenciada em milissegundos.

Usualmente, o ping tem um valor de tempo limite para sua resposta. Se a resposta não é recebida dentro do tempo que se espera, o ping notifica com uma mensagem informando que tal resposta não fora recebida, somente isso significa que existem problemas, mas também pode indicar que recursos de segurança que são capazes de bloquear mensagens estão ativados na rede, por exemplo, o bloqueio por um firewall.

Depois que todas as requisições estejam encaminhadas, o ping exibirá um resumo que ainda inclui a taxa de sucesso ou insucesso e também o tempo médio de ida e volta do pacote até o seu destino.

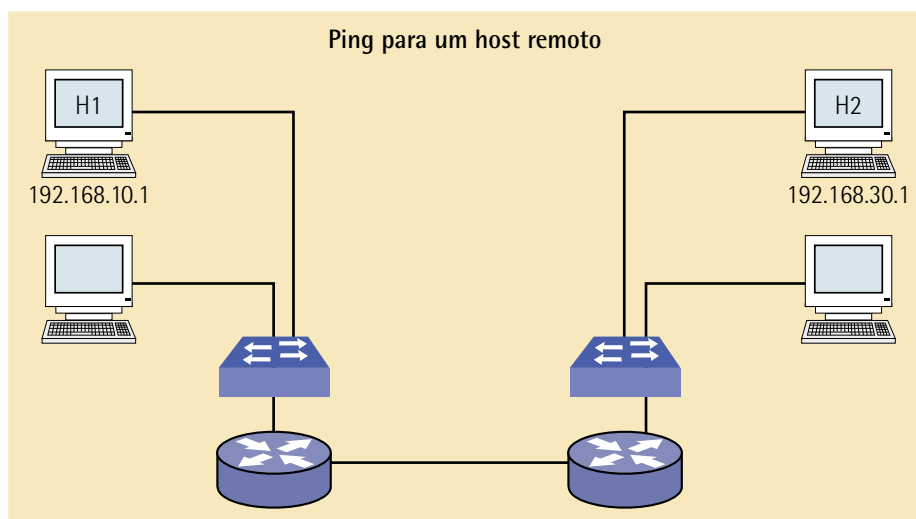


Figura 72 – Comando ping remoto



Saiba mais

Uma nova dica de uma leitura importante para aprofundar seus conhecimentos em protocolos ICMP:

TANENBAUM, A. S. Protocolos de controle da internet: ICMP (Internet Control Message Protocol). In: _____. *Redes de computadores*. 4. ed. São Paulo: Campus, 2003. p. 346.

5.2.8 Ping no loopback local

Existem casos especiais de teste de verificação de conectividade em que podemos usar o ping. Um deles é a aferição de configuração interna de IPv4 ou de IPv6 diretamente no host local. Para realizar tal teste fazemos um ping no endereço loopback local, 127.0.0.1 para IPv4 (::1 para IPv6). A figura a seguir mostra um teste de loopback de IPv4.

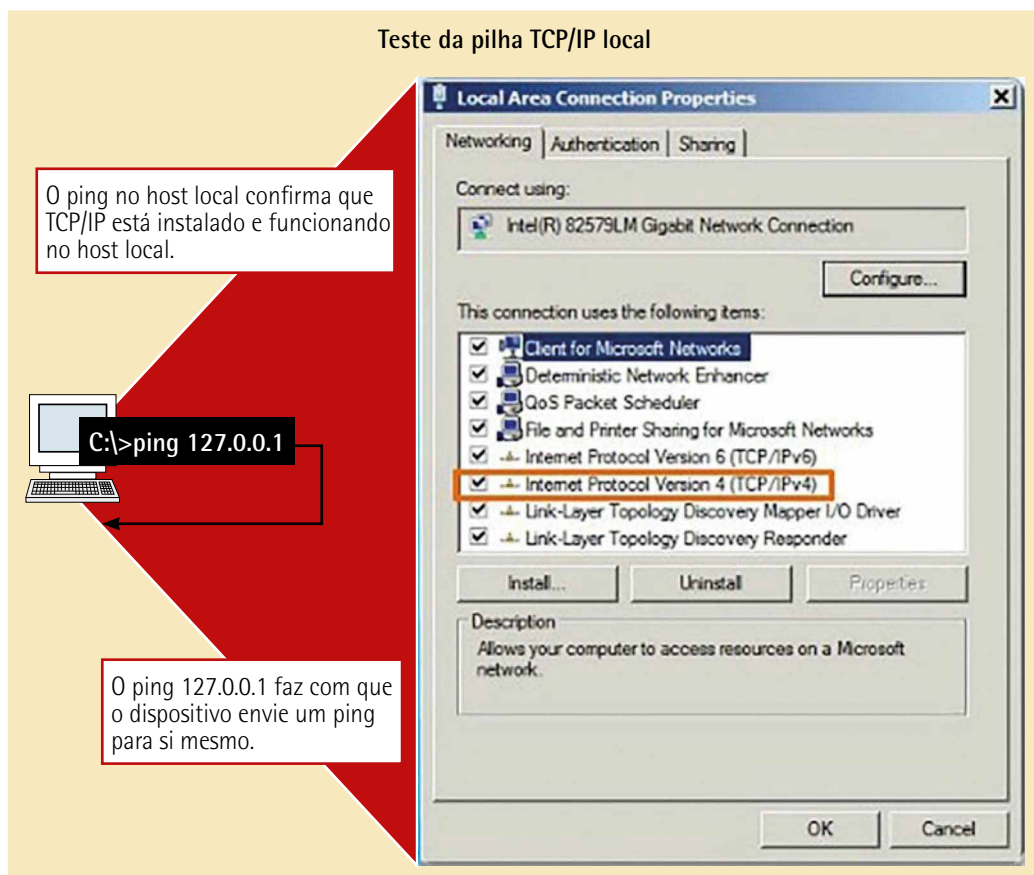


Figura 73 – Teste da pilha TCP/IP local em uma workstation Windows

Uma resposta oriunda de 127.0.0.1 para IPv4 (::1 para IPv6) indica que o IP instalado está em uso correto. Essa resposta vem da camada da rede. Entretanto, ela não significa que os endereços, máscaras ou até mesmo gateways estejam configurados adequadamente, tampouco indica o status da camada inferior da pilha da rede; ela simplesmente testa o IP até a camada de rede. O fato de haver uma mensagem de erro indica se o TCP/IP está operacional ou não no host.

5.2.9 Ping: testando a conectividade com a LAN local

Podemos usar o ping também para testar a capacidade do host de se comunicar com a rede e com outros hosts. Usualmente, basta executar o ping para o endereço IP do gateway do host. O ping no gateway indica que o host e a interface do roteador que serve basicamente como gateway estão operacionais e ativados na rede local.

Para tal teste costumamos usar o endereço do gateway porque o roteador no momento está sempre operacional. Se o endereço do cliente não responder, poderá ser enviado um ping para o endereço IP de outro host da rede local que saiba que este está operacional.

Se o gateway ou algum outro host efetuar a resposta, o host local conseguirá se comunicar pela rede local. Se não houver resposta, mas outro host responder, isso poderá indicar um problema com a interface do roteador que serve como gateway naquele momento.

Outra possibilidade é que o endereço do gateway tenha sido configurado incorretamente na configuração interna do host, ou ainda que a interface do roteador esteja plenamente operacional, mas tenha algum nível de segurança que seja aplicado a ela, e que esta impeça de processar ou responder solicitações ICMP como ping.

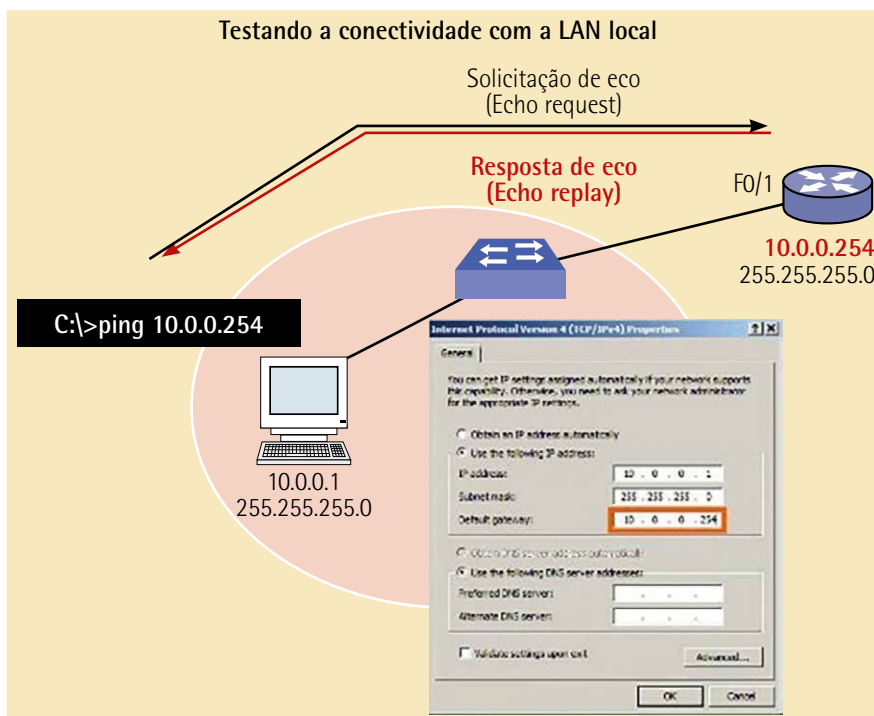


Figura 74 – Testando a conectividade com a LAN local para estações Windows

5.2.10 Ping: testando conectividade remota

O ping também deve ser usado para testar a capacidade de um host local de se comunicar com uma rede interconectada. Esses hosts podem fazer uso do ping a um host IPv4 operacional em uma rede remota, como demonstrado na figura a seguir.

Se correr tudo bem, uma operação de grande parte da rede interconectada poderá ser verificada de, basicamente, todo o segmento interno até as bordas externas. Um ping bem-sucedido pela rede interconectada confirma também a comunicação pela rede local, o funcionamento do roteador que serve como gateway e o funcionamento de todos os outros dispositivos a ela conectados, como outros roteadores que podem estar no caminho entre a rede local e o host remoto.

Ainda, a funcionalidade do host remoto pode ser verificada se ele eventualmente não conseguir comunicação para fora de sua rede local, então ele não responderá à solicitação de ping.



Observação

Há um consenso entre administradores de rede que propositalmente limitam ou até mesmo proíbem a entrada de mensagens ICMP em uma rede corporativa, talvez por isso promova a falta de uma resposta do ping, podendo ser a consequência de determinadas restrições de segurança da infraestrutura.

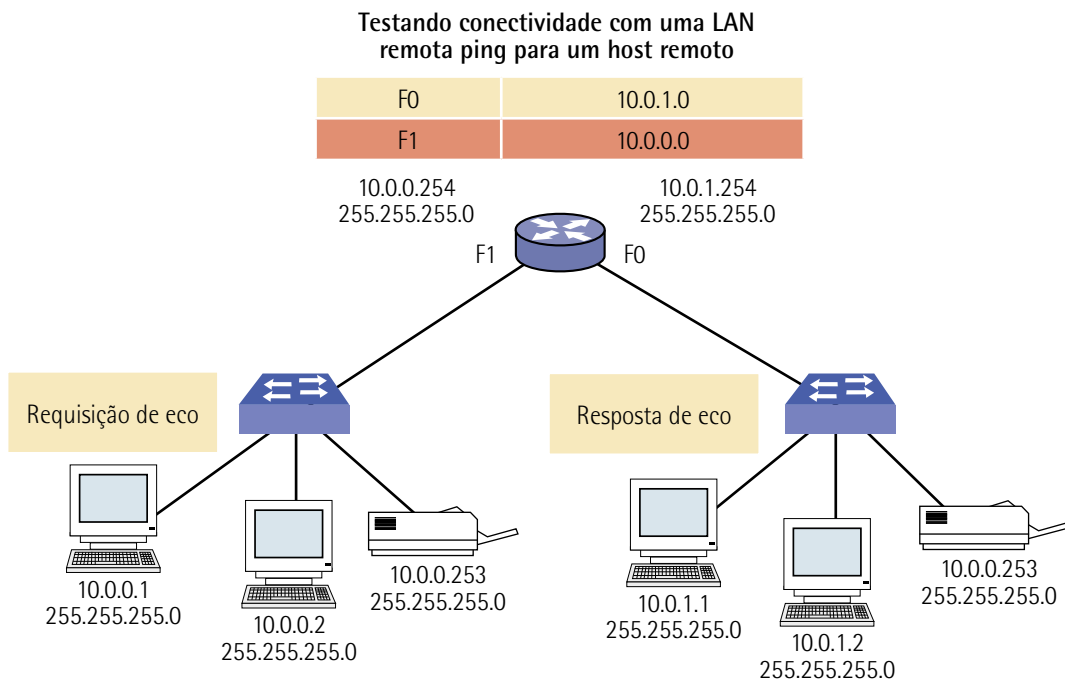


Figura 75 – Testando a conectividade com uma LAN remota

5.2.11 Traceroute: testando o caminho

Sabemos que o ping é usado para testar a comunicação entre dois hosts dentro ou fora de um barramento, porém ele não nos fornece detalhes ou quaisquer informações sobre dispositivos entre os dois equipamentos. Tracerout (tracert) é o utilitário que gera uma lista de saltos que foram sendo atingidos ao longo de um caminho. Esse relatório pode nos dar informações importantes sobre verificação e solução de eventuais erros. Caso os dados atinjam seu destino, o rastreamento lista a interface de cada roteador no caminho entre esses dois hosts. Caso ainda ocorram falhas dos dados em alguns saltos ao longo do caminho, o endereço do último roteador que responder a esse rastreamento nos fornecerá uma indicação de onde está o problema ou as restrições de segurança que foram encontrados ao longo do percurso.



Observação

O limite de saltos de um comando traceroute em protocolo IPv4 é 30.

5.2.12 Tempo de ida e volta (RTT)

Sabemos que o traceroute nos fornece o tempo de vida da ida e da volta de cada salto ao longo do caminho, ele ainda indica se o salto deixou de responder por qualquer questão de segurança. O tempo de ida e volta é o tempo que o pacote leva para alcançar o host remoto e para a resposta desse host chegar até a sua origem. Sempre que o pacote é perdido, um asterisco é usado para representar que esse pacote não foi respondido.

Essas informações são usadas normalmente para localizar um roteador que tem problemas no seu caminho se ainda forem exibidos tempos de resposta muito elevados ou perda de dados de pacotes para um determinado salto, o que também significa que recursos de roteamento ou determinadas conexões podem estar sobrecarregadas.

5.2.13 TTL no IPv4 e limite de saltos no IPv6

O traceroute faz uso da função dos campos TTL (time to live) do IPv4 e do limite de saltos do IPv6 nos cabeçalhos da camada 3, juntamente com mensagens ICMP de tempo excedido.

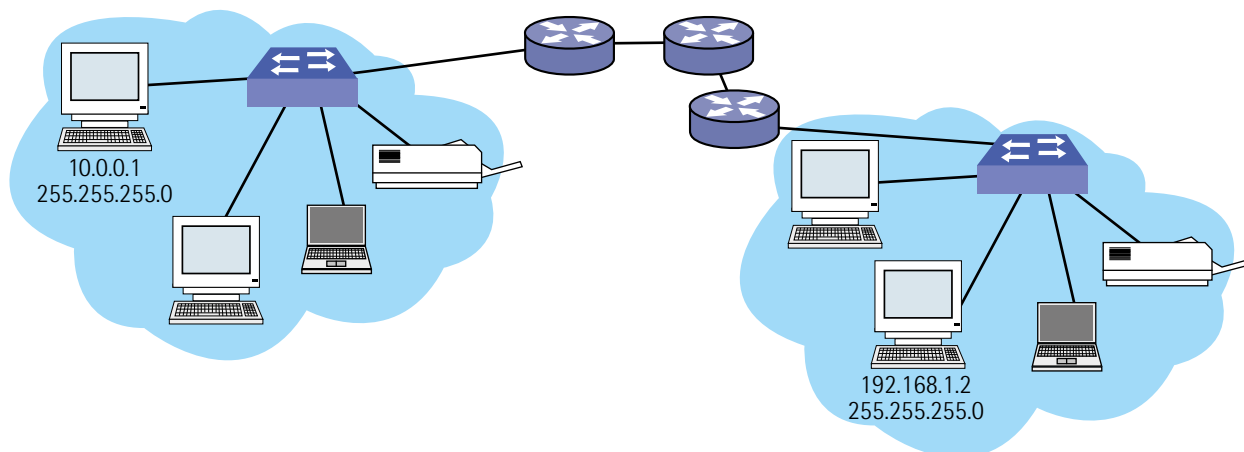
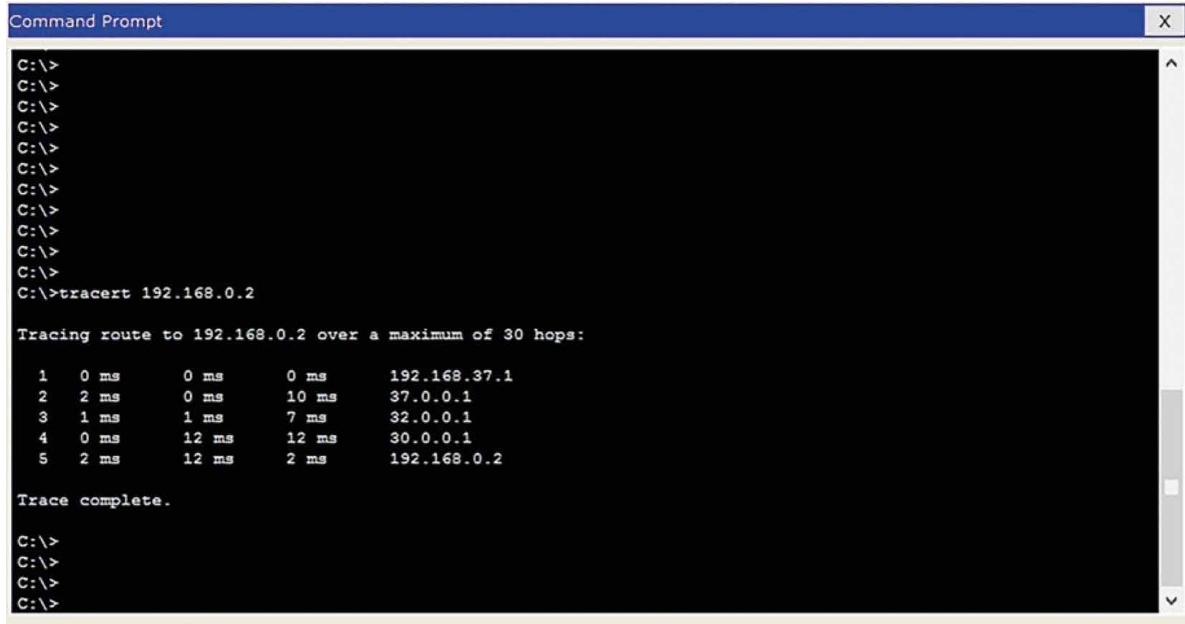


Figura 76 – Executando o traceroute em LAN remota

Analisando a primeira sequência de mensagens enviadas pelo traceroute, haverá um campo TTL com valor 1, isso acontece com o TTL que atribui o tempo limite ao pacote IPv4. E isso sempre acontecerá com o primeiro roteador. Esse roteador responderá com uma mensagem ICMPv4, então o traceroute tem agora o endereço do primeiro salto no código.



```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>tracert 192.168.0.2

Tracing route to 192.168.0.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.37.1
  2  2 ms    0 ms    10 ms   37.0.0.1
  3  1 ms    1 ms    7 ms    32.0.0.1
  4  0 ms    12 ms   12 ms   30.0.0.1
  5  2 ms    12 ms    2 ms   192.168.0.2

Trace complete.

C:\>
C:\>
C:\>
C:\>
```

Figura 77 – Tela de captura do comando traceroute em ambiente Windows

O traceroute aumenta progressivamente os campos TTL (2, 3, 4...) para cada sequência de mensagens recebidas e isso nos dá o rastreamento do endereço de cada salto à medida que a vida útil dos pacotes é excedida ao longo do seu caminho. O campo TTL continua a ser acrescido até alcançar o seu destino ou até atingir um valor máximo predeterminado.

Quando se alcança o destino final, o host responde com a mensagem em ICMP de porta inalcançável ou ainda com uma mensagem ICMP de resposta de eco, em vez de uma mensagem ICMP de tempo excedido.

5.3 O ARP — Address Resolution Protocol

O ARP é um protocolo criado pela RFC826 que adiciona uma funcionalidade que dá permissão aos equipamentos de rede para executar um mapeamento entre os endereços físicos e lógicos em seu segmento.

A atribuição de endereço físico é responsabilidade da camada enlace, porém, em uma comunicação enviada por uma rede, além do endereço lógico, que é o endereço atribuído na camada de rede, por exemplo IPv4 ou IPv6, ainda precisamos saber qual o endereço físico correspondente para que os dados possam ser enviados corretamente, permitindo a entrega dessas informações a seu destinatário.

O ARP, na verdade, é um auxiliar ao protocolo da camada de rede, porém ele é implementado na camada enlace.

No momento que um dispositivo precisa conhecer o endereço físico de outro dispositivo, é construída uma mensagem do tipo broadcast internamente, nessa mensagem é colocado o endereço da camada de rede. Então essa mensagem é enviada pela rede para a descoberta do endereço físico do correspondente. Essa descoberta acontece no momento em que há o retorno de uma mensagem através da rede indicando endereço físico para onde devem ser direcionados os pacotes.

A fim de mitigar o tráfego de broadcast dentro da rede, os equipamentos constroem uma tabela ARP que armazena temporariamente essa associação de endereço físico e lógico dos dispositivos conhecidos dentro da rede. Então, em vez de constantemente enviar uma solicitação de ARP pela rede, o dispositivo antes verifica a sua tabela ARP própria.



Observação

O tempo de vida de uma tabela ARP em cache do seu computador é de 20 minutos.

Veja o fluxograma a seguir, que demonstra o funcionamento do protocolo ARP:

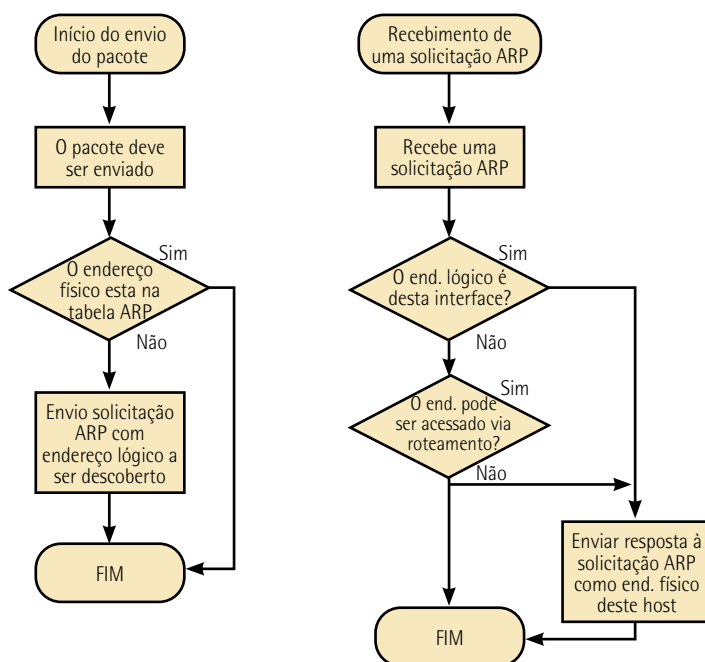


Figura 78 – Fluxograma demonstrativo do funcionamento do protocolo ARP



Lembrete

Endereços IP que são procurados com frequência são armazenados no cache de servidores de DNS mais próximos, fato que ajuda a diminuir o tráfego e o atraso.

Esse armazenamento de endereços é volátil, persiste após um período de tempo, que na maioria dos servidores DNS são de dois dias. Após esse período os dados que estão em cache são descartados.

5.4 Domínios de broadcast

Broadcast é um formato de comunicação existente em uma rede local que tem como principal característica enviar informações para todos os equipamentos que sejam alcançados através desse meio físico.

Esse formato de comunicação é amplamente utilizado por diversos protocolos, como o ARP e o DHCP, além de outros, e ajuda no funcionamento normal das redes. O domínio de broadcast é representado apenas pelos equipamentos que pertencem ao mesmo domínio de broadcast, em relação aos equipamentos. Caso algum deles envie um broadcast, todos os outros receberão e farão conhecimento de seu conteúdo.

A interligação entre equipamentos de um mesmo domínio de broadcast é rigidamente realizada por dispositivos de camada 1, exemplo do cabo coaxial ou hubs, ou ainda por dispositivos de camada 2, como bridges e switches.

A quebra de um domínio broadcast por um dispositivo acontece pelo emprego de qualquer ativo que opera acima da camada 2, por exemplo roteadores, hosts ou switches de camada 3. A figura a seguir mostra um roteador que é separado por dois domínios broadcast.

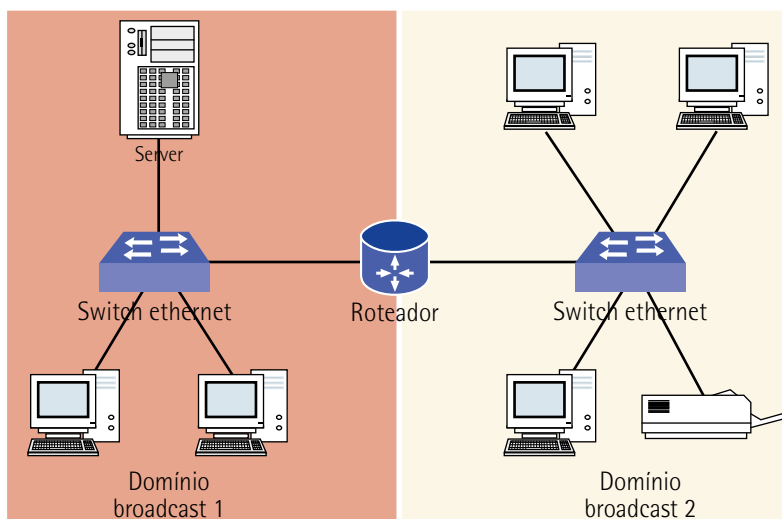


Figura 79 – Dois domínios broadcast separados por um roteador



Saiba mais

Segue leitura indispensável para você saber mais sobre os domínios broadcast:

MAIA, L. P. Virtual LAN (VLAN). In: _____. *Arquitetura de redes de computadores*. 2. ed. Rio de Janeiro: LTC, 2013.

6 AS CAMADAS DE ENLACE E SUAS TOPOLOGIAS

6.1 A camada 2: enlace

A principal tarefa da camada de enlace é fornecer o meio comum para troca de dados entre os equipamentos. Suas principais funções são:

- Permitir que as camadas superiores tenham acesso ao meio físico disponível usando técnicas e métodos de enquadramento que sejam compatíveis com o meio.
- Usar técnicas que permitam acesso ao meio físico.
- Detectar erros nos quadros recebidos, garantindo a integridade das informações no nível mais básico.
- Atribuição do endereço físico MAC Address.
- Promover a criação dos quadros no nível físico da comunicação.

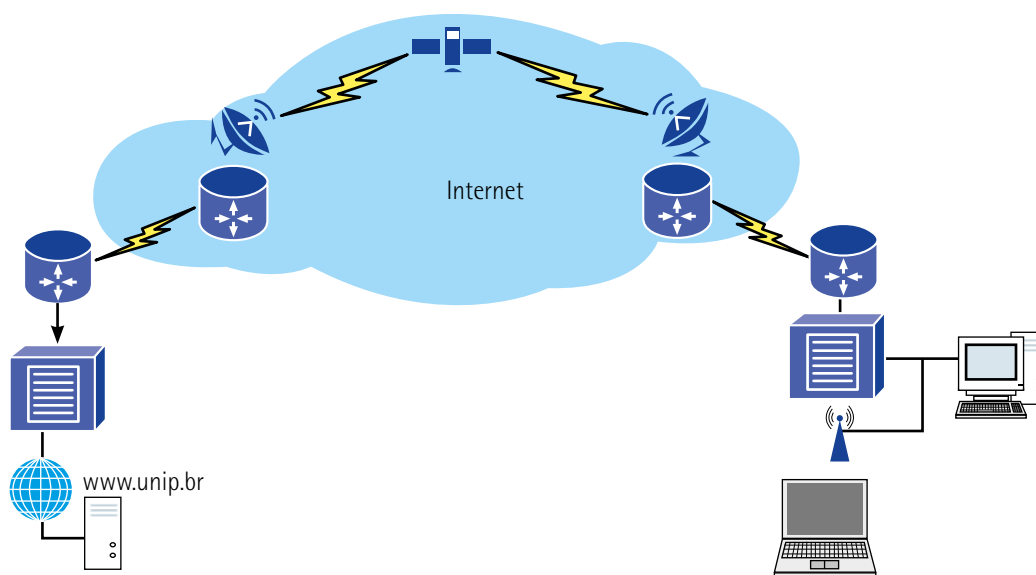


Figura 80 – Representação do funcionamento do acesso à internet

6.2 O PDU (Protocol Data Unit)

É importante dizer que todos os pacotes que são transferidos à camada de rede são produto de um quadro formatado na camada enlace. Esses quadros são conhecidos com PDU (Protocol Data Unit), ou Unidade de Protocolo de Dados, que são associados à comunicação e transferidos entre entidades da mesma camada. Sua construção é singular e simples, tem controle e conteúdo adequados a todos os tipos de modulação e protocolos de camadas superiores.

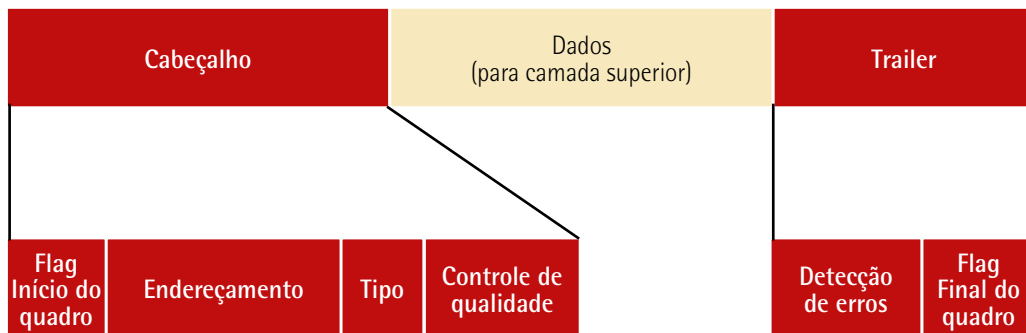


Figura 81 – Detalhamento da composição de um quadro em camada 2

A função de cada campo do PDU:

- Flag de início e final do quadro: limites que identificam e limitam o quadro.
- Endereçamento: endereçamento do quadro, de acordo com o meio utilizado.
- Tipo: tipo da PDU da camada de rede contida no quadro.
- Controle de qualidade: campo que identifica a qualidade.
- Detecção de erros: campo utilizado para validar as informações do quadro. Este campo é calculado no envio do quadro e quando do seu recebimento para verificar se o quadro está íntegro.

6.3 Subcamadas da camada enlace

Em redes cabeadas que usam o protocolo Ethernet, a camada de enlace está integrada com a placa de rede. Isso ocorre porque a camada de enlace está ligada à camada física e precisa estar de acordo com o meio físico. Então, acontece na camada de enlace uma divisão interna que gera duas subcamadas:

- Subcamada LLC (Logical Link Control): é responsável por implementar as informações do quadro que o protocolo de rede precisa. Esta subcamada é a que está mais próxima da camada de rede.
- Subcamada de controle de acesso ao meio (MAC): implementa o endereçamento da camada de enlace de acordo com a tecnologia utilizada e inclui os flags de início e fim do quadro de acordo com a exigência da tecnologia adotada.

6.4 Rede local e suas tecnologias

Na camada de enlace, as regras e arquiteturas de suas tecnologias são descritas por organizações de engenharia como o IEEE, ISO, ANSI e ITU. Nestas descrições, as organizações têm o dever de descrever não somente as características físicas, mas todas as características do acesso ao meio físico ligadas à camada de enlace.

No quadro a seguir, temos as entidades e os comitês que regulamentam essas tecnologias e seus protocolos:

Quadro 1 – Tecnologias e protocolos operados pelos comitês

Comitê	Protocolo
ISO	HDLC – High Level Data Link Control
IEEE	802.2 – LLC
	802.3 – Ethernet
	802.5 – Token Ring
	802.11 – Wireless LAN
ITU	Q.922 – Frame Relay
	Q.921 – ISDN, Integrated Services Digital Network
	HDLC – High Level Data Link Control
ANSI	3T9.5
	ADCCP – Advanced Data Communications Control Protocols

6.5 Acesso ao meio físico

Acontecem diversas implementações da camada de enlace e também diversas implementações para o controle de acesso ao meio físico, que possuem pontos importantes e que se distinguem umas das outras com base na forma como o meio de transmissão é compartilhado e a maneira como a topologia é empregada.

6.5.1 Compartilhamento

Dependendo da tecnologia usada em uma comunicação, a camada de enlace é responsável por definir como essa comunicação vai ocorrer e a forma como serão usados os componentes para que essa comunicação aconteça perfeitamente. Existem dois métodos usados pela camada de enlace para atingir essa realização:

- Método determinístico: em que cada componente da rede possui um tempo determinado dentro do meio físico para transmitir, isso define inclusive quando podemos transmitir e quando não podemos transmitir. Um exemplo para essa situação é o uso da rede Token-Ring.
- Método não determinístico: em que cada componente, ao transmitir uma informação, precisa verificar se o meio físico ainda está disponível para tal. É preciso também verificar se ocorrem

possibilidades de conexão, caso mais de um dispositivo precise transmitir ao mesmo tempo, para evitar que casos de colisão aconteçam na transmissão. Existem dois métodos não determinísticos de acesso que permitem estabelecer, na camada de enlace, o momento de cada um transmitir. O CSMA usa dessas técnicas, que se dividem em outras duas possibilidades:

- CSMA-CD (Carrier Sense Multiple Access/Collision Detection): usa um processo para resolver um impasse no momento da transmissão e recepção dos dados, usado normalmente em redes cabeadas.
- CSMA-CA (Carrier Sense Multiple Access/Collision Avoid): tem a missão de prevenir a colisão antes mesmo que o processo de colisão aconteça, baseado em uma avaliação do meio físico e na reserva de tempo para a transmissão/recepção dos dados. É um método largamente utilizado em redes do tipo sem fio.



Saiba mais

Para você saber mais sobre o Protocolo CSMA e suas variantes, leia:

MAIA, L. P. Protocolo CSMA. In: _____. *Arquitetura de redes de computadores*. 2. ed. Rio de Janeiro: LTC, 2013.

6.6 Topologias

Ao considerar topologias de rede, é preciso avaliar sob duas óticas: a topologia física e a topologia lógica.

A topologia física é a maneira como o meio físico é utilizado para interconectar dispositivos. A topologia lógica é usada para determinar o processo de gerenciamento de acesso ao meio físico. As topologias lógicas mais comuns são do tipo ponto a ponto, ponto a multiponto e anel.

A **topologia ponto a ponto** estabelece a conexão de dois pontos diretamente. Nessa situação, o protocolo da camada de enlace é muito mais simples, pois os dados são destinados diretamente de um equipamento ao outro.



Figura 82 – Topologia ponto a ponto

A **topologia ponto a multiponto** conecta vários pontos utilizando um mesmo meio físico. Os dados de um único equipamento podem ser colocados na rede por vez. Caso mais de um equipamento precise

transmitir simultaneamente, um dos dois métodos de controle de acesso deverá ser usado (CSMA/CD ou CSMA/CA).

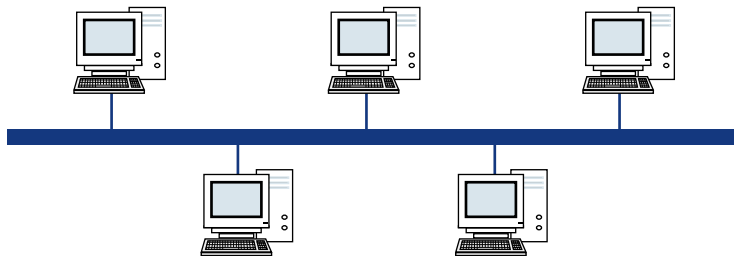


Figura 83 – Acesso ponto a multiponto

Na **topologia anel**, todos os equipamentos de rede são interligados no formato de anel. Os equipamentos recebem os quadros na rede e verificam se são endereçados a eles dentro do meio físico, caso não sejam, eles enviam ao próximo equipamento. O processo de transmissão é controlado por um token (ficha), que irá indicar quando cada equipamento poderá transmitir.

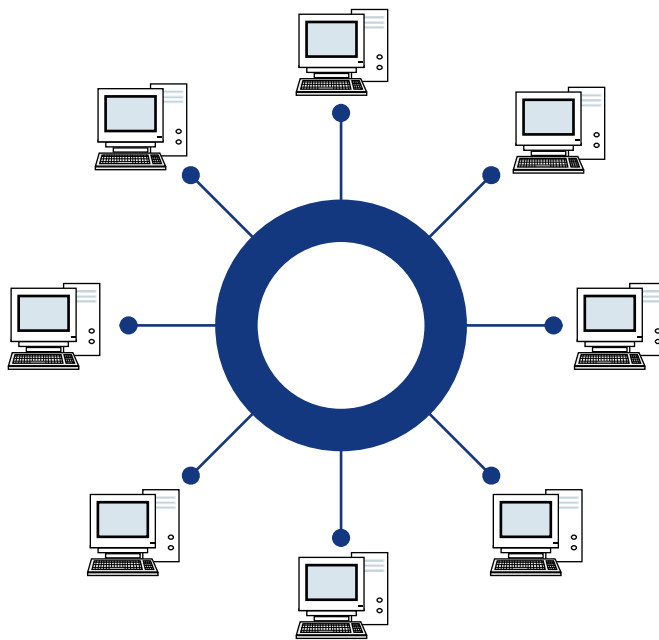


Figura 84 – Topologia em anel

6.7 Ethernet (IE 802.3) e suas variantes

Em 1980 a família de padrões Ethernet estreou no mercado, quando um consórcio de empresas (Digital Equipment Corporation, Intel e Xerox) introduziram este padrão.

Já em 1985, o comitê IEEE (Institute of Electrical and Electronics Engineers) publica um conjunto de padrões que definem o início de todos os protocolos padrão Ethernet. Tudo começa com o padrão 802, sendo que o padrão 802.3 atendia às camadas 1 e 2 do modelo de referência OSI.

O padrão Ethernet divide as funções da camada em duas subcamadas:

- Subcamada de modelo lógico (LLC):
 - Conexão com as camadas superiores.
 - Encapsula o pacote da camada de rede.
 - Identifica o protocolo da camada de rede.
 - Consegue permanecer independente das questões físicas.
- Subcamada de controle de acesso aos meios:
 - Delimitação do quadro, de acordo com o dispositivo físico.
 - Endereçamento.
 - Detecção de erros.
 - Gerência do controle de acesso aos meios (transmissão, colisão etc.).

Para o IEEE, o padrão 802.2 define as funções da subcamada de modelo lógico, e o padrão 802.3 define a subcamada de controle de acesso aos meios e a todas as funções da camada física.

Desde o começo, o padrão Ethernet usa como topologia lógica o barramento com multiacesso e usa como método de controle de acesso o CSMA/CD (Carrier Sense Multiple Access/Collision Detection).

Atualmente, mesmo com todas as evoluções existentes na Ethernet, a topologia lógica considerada é o barramento com multiacesso. Sabendo dos problemas decorrentes desse formato de acesso ao meio, a Ethernet vem se moldando para atender às necessidades do mercado e à crescente demanda de altas velocidades em redes LAN.

As principais diferenças da rede Ethernet em relação a outras tecnologias e que garantem seu sucesso são:

- Baixo custo de instalação e manutenção.
- Confiabilidade.
- Incorporação de novas tecnologias sem a necessidade de trocar toda a rede (preservação dos investimentos realizados).

Observando os principais tipos de rede Ethernet que existem, podemos ver a evolução tecnológica que ocorreu nas redes LAN.

- Cabeamento coaxial: todos os equipamentos conectados em um mesmo barramento:
 - Thicknet (10BASE5): opera com cabo coaxial grosso que se estende até 500 metros.
 - Thinnet (10BASE2): cabo coaxial fino que opera a distância de cabeamento de 185 metros.
- Cabeamento UTP: conectado em um ativo de rede (hub, switch):
 - 10BASE-TX: usa o hub como ponto central de distribuição aos cabos UTPs; as transferências são half-duplex, ainda, o equipamento envia ou recebe em um dado momento e não pode realizar as duas funções simultaneamente. Largura de banda de 10 Mbps.
 - 100BASE-TX: opera com transferências full-duplex de 100 Mbps, ainda, envia e recebe dados simultaneamente, porém com largura de banda de 100 Mbps.
 - 1000BASE-TX: opera transferências full-duplex de 1.000 Mbps, ainda, envia e recebe dados simultaneamente, porém com largura de banda de 1000 Mbps.
 - 10GBASE-T: operam transferências de 10 Gbps em cabeamento UTP.
- Cabeamento fibra ótica:
 - 100BASE-FX: opera transferência de 100 Mbps.
 - 1000BASE-LX: opera transferência de 1.000 Mbps.
 - 10GBASE-LX4: opera transferência de 10 Gbps.

As redes de Ethernet são conhecidas por outros nomes, de acordo com a velocidade de transmissão. Confira na tabela a seguir:

Tabela 11 – Padrões Ethernet

Velocidade em megabits por segundo	Padrão
10	Ethernet
100	FastEthernet
1.000	GigabitEthernet
10.000	10 GigabitEthernet

6.8 Domínios de colisões

Sabemos que o padrão Ethernet trabalha com o protocolo CSMA/CD, seu ponto forte é a utilização de um meio compartilhado para otimizar os recursos na rede. Porém, o uso desse protocolo gera efeitos colaterais, em que todos os equipamentos que estiverem no mesmo barramento estão sujeitos à colisão de suas tentativas de transferência.

Os equipamentos que estiverem acessando um mesmo meio compartilhado estão sujeitos à colisão entre si e são considerados ocupando o mesmo domínio de colisão. Avaliando as possibilidades de interconexão entre esses equipamentos, podemos representar os seguintes exemplos de domínio de colisão nas duas figuras a seguir:

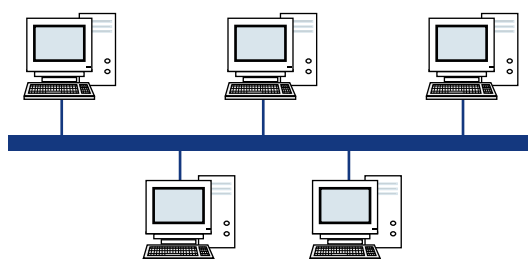


Figura 85 – Domínio de colisão em formato barramento

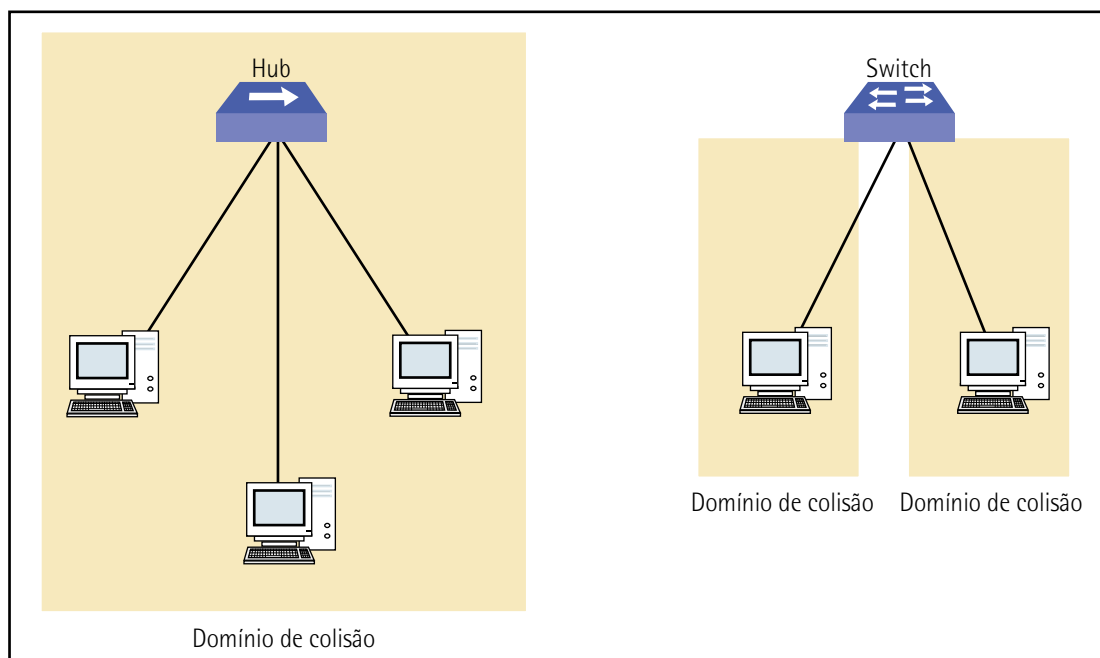


Figura 86 – Comparando domínio de colisão usando hub e switch



Resumo

Esta unidade foi importante porque começamos a desvendar os mistérios da camada de enlace, passando por conceitos importantes da representatividade do mundo lógico das redes de computadores.

Aprendermos que o ICMP é um protocolo importante que opera conjuntamente com o protocolo IP. Atua na camada 3 do modelo OSI porque ele não é usado especificamente para transmissão de dados, mas sim como um protocolo de auxílio para o funcionamento da camada 3.

Aplicamos os fundamentos das ferramentas de diagnóstico como ping e traceroute nos roteadores e nas estações de trabalho. Foram abordados como elementos do ICMP. Descobrimos ainda que ICMP é o mecanismo que informa os erros de uma transmissão de dados e dá possibilidade para os roteadores manterem informadas as entidades transmissoras sobre as diferentes causas de erro.

Fizemos uma comparação sistêmica sobre as versões de ICMP versão 4 e do ICMP versão 6, falamos sobre a confiabilidade do protocolo IP e toda a suíte de protocolos que o IP nos propicia.

Aprendemos sobre multicast, anycast, sobre a detecção de endereçamentos duplicados usando o IP versão 6. Executamos testes de verificação de link local e encontramos os limites de tempo dos pacotes. Abordamos profundamente o assunto domínio de broadcast.

Por fim, acessamos a camada de enlace, avaliamos o PDU, entendemos todos os componentes do PDU e suas subcamadas. Aprendemos sobre redes locais e suas tecnologias pelos comitês ITU, ISO, IEEE. Entendemos as mecânicas de compartilhamento com o protocolo CSMA, e ainda avaliamos as topologias ponto a ponto, multiponto e anel.

Entendemos os processos do protocolo Ethernet 802.3 da forma como conceituamos barramento, cabeamento, fibra ótica, meios metálicos e domínios de colisão.



Exercícios

Questão 1. O ICMP é um protocolo que, conjuntamente com o IP, opera na camada 3 do modelo OSI. Entretanto, não é usado especificamente para transmissão dos dados, mas sim como protocolo de controle que auxilia no bom funcionamento do protocolo IP. A funcionalidade efetiva do ICMP permite que equipamentos roteadores e ativos de rede interligados possam informar erros ou quaisquer problemas inesperados ocorridos durante uma transmissão de dados.

Com relação ao ICMP, algumas das mensagens mais comuns são:

- I – Confirmação de host.
- II – Destino ou serviço inalcançável.
- III – Tempo excedido.

Estão corretas, apenas, as mensagens:

- A) I e II.
- B) II e III.
- C) I, II e III.
- D) I e III.
- E) III.

Resposta correta: alternativa C.

Análise das mensagens

- I – Mensagem correta

Justificativa: uma mensagem proveniente do eco ICMP pode ser usada para determinar se o host está ou não operacional. O host local envia uma solicitação de eco no padrão ICMP (ECHO REQUEST) para um host, se o host estiver ativo e disponível, o host de destino enviará uma resposta de eco (ECHO REPLY).

- II – Mensagem correta

Justificativa: no momento que o host ou gateway recebe um pacote e este não pode ser entregue, ele pode fazer uso de uma mensagem ICMP de destino inalcançável para notificar à origem do datagrama

que o destino ou serviço está inalcançável. Essa mensagem conterá um código que indica o motivo pelo qual não foi possível entregar o pacote.

III – Mensagem correta

Justificativa: uma mensagem ICMPv4 de tempo excedido é usada por um roteador para indicar que um determinado pacote não pode ser encaminhado porque seu tempo de vida útil TTL (time to live) foi reduzido a zero. Caso o roteador receba um novo pacote, o campo TTL (time to live) do pacote IPv4 diminui para zero, ele então descartará o pacote e enviará uma mensagem de tempo excedido para o host da origem. No caso do ICMPv6, este roteador enviará uma mensagem de tempo excedido, caso o roteador não esteja conseguindo encaminhar um pacote IPv6, basicamente porque o pacote expirou. O IPv6 não tem um campo TTL (time o live) ativo, em vez disso, ele usa um campo referente ao limite de saltos para determinar se o pacote expirou ou não.

Questão 2. Ping é um utilitário que usa o protocolo ICMP para testar a conectividade entre equipamentos. É um comando disponível praticamente em todos os sistemas operacionais.

Assinale a alternativa correta. O funcionamento do ping consiste:

- A) No envio de pacotes para o equipamento de destino e na "escuta" das respostas.
- B) No uso do campo time to live (TTL) do pacote IPv4 destinado a limitar o tempo de vida dele. Esse valor é decrementado a cada vez que o pacote é encaminhado por um roteador.
- C) Em adicionar uma funcionalidade que dá permissão aos equipamentos de rede para executar um mapeamento entre os endereços físicos e lógicos em seu segmento.
- D) Na comunicação existente em uma rede local que tem como principal característica enviar informações para todos os equipamentos que sejam alcançados através desse meio físico.
- E) Na resposta do pong.

Resposta correta: alternativa A.

Análise das alternativas

A) Alternativa correta.

Justificativa: o ping é o utilitário de teste que utiliza o protocolo ICMP além de suas mensagens de solicitação de eco e de uma resposta de eco para aferir a conectividade entre dois hosts. O ping tem funcionalidade garantida com hosts IPv4 e hosts IPv6.

B) Alternativa incorreta.

Justificativa: essa é uma característica do funcionamento do traceroute.

