

# Network Based Application Recognition RTP Payload Classification

## Network Based Application Recognition Overview

Enterprise and Service Provider customers develop, maintain and enhance their networking infrastructure to support applications and protocols. Their networks run a wide range of applications, depending on business objectives and numerous other criteria. These applications have certain requirements and expectations from the network infrastructure, which are often specified in terms of bandwidth, delay, jitter, throughput, and packet loss.

The intention of IP Quality of Service (QoS) is to provide appropriate network resources or Service Level Agreements (SLAs) to applications, and to maximize the ROI on the network infrastructure. Network resources must be distributed in a manner that ensures the non-critical applications do not hamper the performance of critical applications.

Customers typically deploy IP QoS by defining five or six different classes of service using various classification techniques available in the Cisco IOS® QoS framework: Real Time Voice, Real Time Video, Interactive, Transactional, Streaming Video, and Best Effort.

Cisco IOS QoS class-based tools for Marking, Congestion Management, Congestion Avoidance, Link Efficiency

mechanisms and Policing and Shaping can then be used to provide the network resources to guarantee the desired performances for these applications.

Classification is therefore a crucial first step in QoS deployment primarily because customers must:

- Identify various applications and protocols running on their networks
- Understand the application behavior with respect to the available network resources
- Identify the mission-critical and non-critical applications
- Categorize the application and protocols in the different classes of service accordingly

Network Based Application Recognition (nBAR) is an intelligent classification engine in Cisco IOS Software that can recognize a wide variety of applications, including Web-based and client/server applications. Once the applications are recognized, the network can invoke required services for that particular application. With the rapid deployment of QoS, newer requirements for packet classification have emerged.

nBAR performs the following two functions:

- Identification of applications and protocols (Layer 4 to Layer 7)
- Protocol discovery



## Identification of Applications and Protocols (Layer 4 to Layer 7)

nBAR can classify applications that use:

- Statically assigned TCP and UDP port numbers
- Non-UDP and non-TCP IP protocols
- Dynamically assigned TCP and UCP port numbers negotiated during connection establishment
  - Stateful inspection is required for classification of such applications and protocols. This is the ability to discover data connections that will be classified by passing the control connections over which the data connection port assignments are made.
- Sub-port classification: classification of HTTP (URLs, mime or host names) and Citrix applications (ICA traffic based on published application name)
- Classification based on deep packet inspection and multiple application specific attributes. RTP Payload Classification is based on this algorithm, in which the packet is classified as RTP, based on multiple attributes in the RTP header.

## Protocol Discovery

Protocol Discovery is a commonly used nBAR feature that collects application and protocol statistics (ie: packet counts, byte counts and bit rates) per interface. QoS Device Manager (QDM) graphically displays this information, and the same functionality will soon be incorporated into QoS Policy Manager (QPM).

nBAR Protocol Discovery MIBs are currently under development (Cisco IOS Software Release 12.[6<sup>th</sup>]T). The most important function of Protocol Discovery is monitoring. When it is deployed with QDM, it enables customers to generate real-time statistics on the applications in their network. It also gives them an idea of the traffic distribution at key points in the network.

Therefore, nBAR is an application-aware intelligent classification engine that provides real time statistics. It will soon also provide historical statistics, based on the introduction of the Protocol Discovery MIBs. nBAR is an important element in many Cisco initiatives, including Architecture for Voice, Video, and Integrated Data (AVVID), Content Delivery Networks, and Storage Area Networks. It has the application-specific intelligence to classify traffic, and is tightly integrated into the QoS solution.

nBAR plays an important role in the security arena, although it is not intended to be a security tool, it works with other QoS class-based policing features to block certain viruses. Because of its multiple inherent capabilities to identify applications, nBAR, along with other QoS features can deny or limit network resources to rogue or misbehaving applications.



## RTP Overview

RTP is a widely used packet format for multimedia data streams. It can also be used for media-on-demand, and for interactive services (ie: Internet telephony). The RTP protocol framework provides end-to-end delivery services for data with real time characteristics. The information carried in the RTP header includes payload type identification, time stamping, sequence numbers, source identification, and reception quality feedback. RTP streams consist of two parts: data and control:

- *Control*: Real-time Transport Control Protocol (RTCP)
- *Data*: a thin protocol providing support for applications with real-time properties; includes timing reconstruction, loss detection, security and content identification

Per the RTP Protocol definition, even UDP port numbers carry RTP data, while the next higher, odd, port number carry corresponding RTCP packets. The payload type (PT) in the RTP header essentially indicates the CODEC used by the application.

## RTP Payload Types

Table 1 shows the set of standard encoding for audio and video traffic as defined by IANA and lists their static payload type value for the Payload Type (PT) field of the RTP data header.

Table 1 RTP Payload Types

PT	Encoding name	Audio/Video (A/V)	Clock Rate (Hz)	Channels (audio)
0	PCMU	A	8000	1
1	1016	A	8000	1
2	G726-32	A	8000	1
3	GSM	A	8000	1
4	G723	A	8000	1
5	DVI4	A	8000	1
6	DVI4	A	16000	1
7	LPC	A	8000	1
8	PCMA	A	8000	1
9	G722	A	8000	1
10	L16	A	44100	2
11	L16	A	44100	1
12	QCELP	A	8000	1
13	CN	A	8000	1
14	MPA	A	90000	
15	G728	A	8000	1



Table 1 RTP Payload Types (Continued)

PT	Encoding	Audio/Video	Clock Rate	Channels
16	DVI4	A	11025	1
17	DVI4	A	22050	1
18	G729	A	8000	1
19	reserved	A		
20	unassigned	A		
21	unassigned	A		
22	unassigned	A		
23	unassigned	A		
dyn	GSM-HR	A	8000	1
dyn	GSM-EFR	A	8000	1
dyn	L8	A	var.	var.
dyn	RED	A		
dyn	VDVI	A	var.	1
24	unassigned	V		
25	CelB	V	90000	
26	JPEG	V	90000	
27	unassigned	V		
28	nv	V	90000	
29	unassigned	V		
30	unassigned	V		
31	H261	V	90000	
32	MPV	V	90000	
33	MP2T	AV	90000	
34	H263	V	90000	
35–71	unassigned			
72–76	reserved for RTCP conflict avoidance			
77–95	unassigned			
96–127	dynamic			

Additionally, end RTP hosts may define payload type values dynamically in the range of 96–127.



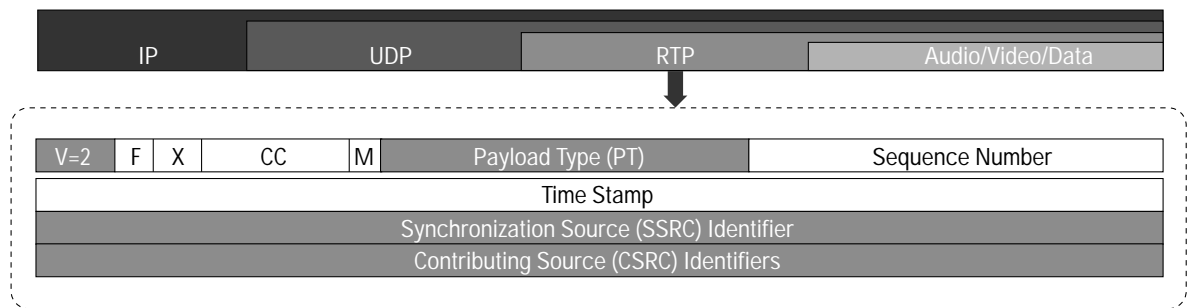
*Example:*

- Session directory could specify that for a given session, payload type 96 indicates G721 encoding and an 8KHz sampling rate.
- Other payload type numbers (34 to 95) are currently either unassigned or reserved.
- The payload type can also be negotiated by the session participants, based on either:
  - Capabilities of the applications used or
  - Previously established agreements between the human participants

Classification of RTP Payload Types using nBAR

nBAR RTP payload classification not only allows the router to statefully identify real time audio and video traffic, but it can also differentiate RTP streams on the basis of specific audio and video CODECs used. nBAR RTP Payload Classification looks deeper into the RTP header to classify RTP traffic for voice and video based on the payload type used (ie: G.711, G.729, and MPEG). The packet is classified as RTP based on multiple attributes in the RTP header, rather than even UDP port numbers alone.

Figure 1. nBAR RTP Payload Type Classification



Why nBAR RTP Payload Classification

While placing voice and video on a network, adequate bandwidth must exist to meet the service needs of these applications. Classification and Marking of the traffic should be performed as close to the edge of the network as possible. The marked DSCP values can then classify, condition, and define the per-hop behavior of each traffic class of traffic within the Diffserv domain.

Cisco IOS Software currently offers many methods for the classification of voice and video traffic. The advantages and disadvantages of each feature are listed below.

1. Match ip rtp

This command matches IP RTP packets that fall within the specified UDP port range. The “match ip rtp” feature matches UDP packets destined to all even port numbers within the specified range. Its limitation is that it will match any UDP packet using an even port number that falls within the range configured. There is a risk that another application could use UDP ports that fall in the same range, as specified by the “match ip rtp” match criteria. This application traffic will now be queued in the Low Latency queue with the delay sensitive voice traffic, and might hamper the quality of voice calls. It is therefore very useful to have a classification engine that can classify applications above the port number criteria.



## 2. Ip dscp and ip precedence

Various applications and end devices (ie: IP Phones and Polycom Video units) can set their DSCP values. The router can now use this specific DSCP, or Precedence, value as classification criteria for voice and video streams. However, a danger does always exist, because another end user or application could, deliberately or accidentally, mark their packets with the same DSCP or Precedence value.

## 3. Access lists

Access lists can classify RTP packets, based on source or destination IP addresses, and UDP port number range but do not provide a granular way to classify RTP streams. Again, there is a risk of another application inadvertently matching the access-list criteria for identification of voice and video traffic, resulting in potential theft of service for these service classes. Also, access-lists do not provide classification statistics that are available with nBAR. nBAR thus provides more granular and application-specific matching criteria than access lists.

## 4. nBAR RTP Payload Classification

This feature expands the RTP traffic-matching capabilities of an nBAR-enabled router by looking deeper into the RTP header to check for RTP specific parameters instead of relying on even UDP port numbers alone

This feature also addresses the challenge of distinguishing RTP packets from different applications based on their payload types or CODECS. The space for payload types is limited, so only very common encodings are assigned static types. These are typically audio and video encodings that have been “blessed” by international standardization bodies, such as the G. series of ITU-T audio encodings (see Table 1). Dynamic payload types map an RTP payload type to an audio and video encoding for the duration of a session. Different members of a session could use different mappings if needed. As shown in the above table, Dynamic payload types use the PT range 96–127.

There are multiple encodings defined by the A/V profile that use dynamic payload types, including GSM-HR, RED, VDVI, L8, MP2P and BMPEG Codecs. nBAR RTP Payload type classification provides a powerful means of classifying the applications based on their static or dynamic payload type.

## Configuration

To configure nBAR to match RTP traffic, use the match protocol rtp command within the class map configuration.  
`match protocol rtp [audio | video | payload-type payload-string]`

The syntax description is as follows:

**Audio**—Specifies matching for payload type values 0–23. Table 1 shows that these values are reserved for audio traffic.

**Video**—Specifies matching for payload type value 24–33. These values are reserved for video traffic (Table 1).

**Payload-Type**—This matches traffic belonging to a specific payload type value, thus providing more granularity than the audio and video options mentioned above.

**Payload-string**—This user-defined string can match against all the specific RTP payload type values from 0–127. Use commas to separate payload type values, and use hyphens to indicate a range of payload type values.



```
Router(config)#class-map nbar_rtp
Router(config-cmap)#match protocol rtp ?
```

```
audio          Match voice packets
payload-type   Match an explicit PT - payload type
video         Match video packets
<cr>
```

Entering the “match protocol rtp” command without any other keywords establishes all RTP traffic as a successful match criteria.

### Sample Configuration Examples

a. The following example configures nBAR to match all RTP traffic:

```
class-map nbar_rtp
  match protocol rtp
```

b. The following example configures nBAR to match RTP traffic with the payload-types 0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 64

```
class-map nbar_rtp
  match protocol rtp payload-type "0, 1, 4 - 0x10, 10001b - 10010b, 64"
```

To use hexadecimal notation, prepend “0x” to each value. To use binary notation, append a “b” after each value.

### RTP Usage Scenarios

Several RTP applications include audio and video tools, and diagnostic tools, such as traffic monitors. RTP is the transport of choice for telephone calls and streaming audio or video. The International Telecommunication Union employs it in the multimedia communications standard H.323, which is used by the real-time streaming protocol (RTSP). There are thousands of users of these applications. The current Internet cannot yet support the full potential demand for real-time services. High-bandwidth services using RTP, including video, have the potential to seriously degrade the quality of service of other network services. When coupled with the ever-present requirement that critical enterprise applications perform optimally, the days of best effort service are rapidly disappearing.

Additionally, voice and video have stringent QoS requirements that the underlying network infrastructure must meet. If these services are not given preferential treatment, it could result in rapid quality degradation to the point of being unusable.

Following are they key requirements for Voice traffic:

- One-way latency should be lesser than 150 ms
- Packet Loss should be less than 0.1%
- Average jitter should be less than 40 ms
- Depending on the CODEC used, bandwidth requirement per call can range from 22 Kbps to 106 Kbps. This will also vary based on the L2 technology used i.e. calls over ATM will have higher L2 overhead than ones made using PPP or FR
- At least 3% of total bandwidth allocation made for voice must be reserved for voice control traffic

There are two main types of video applications:

- Streaming video: non-Real Time (ie: IP/TV; VoD)



- Interactive video: Real Time applications (ie: Video Conferencing)

Following are they key requirements for Streaming Video Applications:

- Latency should be no more than 4-5 seconds
- Packet Loss should be less than 1%
- There are no significant jitter requirements
- Bandwidth requirements depend on the CODEC and the application rate

Streaming video applications have more lenient QoS requirements, as they are delay insensitive (the video can take several seconds to 'cue-up'), and are essentially jitter insensitive (due to large application buffers). Some, including E-Learning applications, may contain valuable content, increasing their sensitivity to packet drops and losses.

Following are the key requirements for Interactive Video Applications:

- One-way latency should be lesser than 200 ms.
- Packet Loss should be less than 1%
- Average jitter should be less than 112 ms.
- The minimum bandwidth guarantees made must be at least 20% more than what is actually required as this will ensure faster scheduling of video packets on the wire.

Basically, video conferencing and voice have similar QoS requirements, in terms of latency, loss and jitter; however, the traffic patterns differ radically . For example, video conferencing traffic has varying packet sizes and extremely variable packet rates, while voice traffic travels is at a fixed rate with small packet sizes.

Additional situations can use RTP payload type to classify applications:

1. *Audio and Video Conference*: Both audio and video media are used in a conference, and are transmitted as separate RTP sessions with no direct coupling at the RTP level. In low bandwidth areas, the PT can be used to allow participants to receive only one medium, if they so choose.
2. *Interactive Media Applications*: RTP may be the base transport protocol for non-voice and video interactive media applications (ie: shared whiteboards or text editor, a distributed presentation tool, or a networked multiplayer game).
3. A telephone answering machine application needs to be able to receive a media stream from an RTP session and store it in a file.
4. An application that records a conversation or conference must be able to receive a media stream from an RTP session. It must render it on the console and store it in a file.
5. *Fax over IP (FoIP)*: enables the interworking of standard fax machines with packet networks using either a realtime or a store and forward approach. The fax image is extracted from an analog signal and carried as digital data over the packet network. QoS mechanisms must be enforced to mitigate the effect of delay across the network, and to minimize jitter and avoid packet loss. Packet loss can severely hamper the performance of this application, because lost information could result in a failure of transmission by the fax protocol.

nBAR RTP Payload Type Classification can be used to identify these various applications and categorize them. The service guarantees for each of these application classes can now be met in terms of jitter, latency, and packet loss using QoS features: Marking, Congestion Management, Congestion Avoidance, Policing, and Shaping.

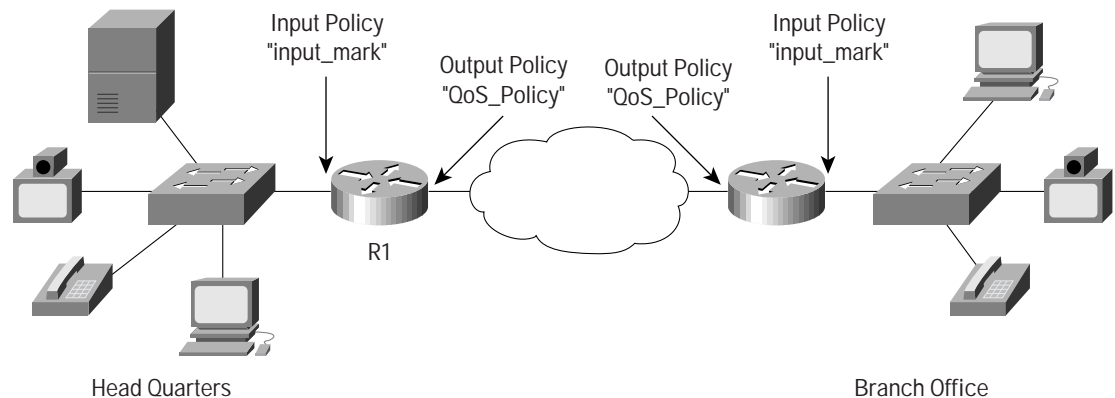


## Configuration Examples for Voice and Video QoS using nBAR RTP Payload Classification

Consider a scenario in which headquarters and remote branch offices send each other voice, video, and data over WAN links.

Video traffic includes real time video conferencing as well as VODs for the e-learning portal. The e-learning application server uses Bundled MPEG codec that is configured to dynamically negotiate RTP payload Type 97 for the sessions. If there was no QoS data traffic, the streaming BMPEG traffic could starve the real time traffic and interactive data of the needed bandwidth. nBAR can identify and classify these multiple types of traffic, while QoS mechanisms (ie: Marking and Queuing) can mark and prioritize the mission-critical traffic through the network.

Figure 2. nBAR for Voice, Video and Data QoS Deployment



```
Class-map voice
  Match rtp protocol audio
Class-map video-conferencing
  Match rtp protocol video
Class-map e-learning-vod
  Match rtp payload-type "97"
Class-map transactional
  Match protocol notes
Class-map interactive
  Match protocol citrix
```

```
Policy-map input_mark
  Class voice
    Set ip dscp ef
  Class video-conferencing
    Set ip dscp af41
  Class e-learning-vod
    Set ip dscp af11
  Class transactional
    Set ip dscp af21
```



```
Class interactive
  Set ip dscp af31

Interface Input
  Service-policy input input_mark

Class-map voice
  Match ip dscp ef
Class-map video-conferencing
  Match ip dscp af41
Class-map e-learning-vod
  Match ip dscp af11
Class-map transactional
  Match ip dscp af21
Class-map interactive
  Match ip dscp af31

Policy-map QoS-Policy
  Class voice
    Priority percent 10
  Class video-conferencing
    Bandwidth remaining percent 20
  Class e-learning-vod
    Bandwidth remaining percent 35
  Class transactional
    Bandwidth remaining percent 15
  Class interactive
    Bandwidth remaining percent 30
  Class class-default
    Fair-queue

Interface Output
  Service-policy output QoS-Policy
```

## MIB Support

Support for the nBAR Protocol Discovery MIB is currently scheduled for the Cisco IOS Software Release 12.2(6<sup>th</sup>)T.

## Summary

RTP payload is the data transported by RTP in a packet. RTP Payload Classification is a powerful tool that provides customers with a stateful mechanism to identify audio and video traffic in their network. It also includes the ability to differentiate RTP traffic based on audio and video codecs that the various applications use. The PT classification also enables identification of non-voice and video applications using RTP as the packet format.

## Caveats

- No support exists for classifying the RTCP control traffic in a RTP session
- CEF is a prerequisite for nBAR
- nBAR is not supported in the PXF and Multicast switching paths

## Cisco IOS Software Support

Cisco added this enhancement to nBAR in Cisco IOS Software Release 12.2(8)T. It is also available in Cisco IOS Software Release 12.1(11b)E.

## Supported Platforms

For a list of all platforms that currently support nBAR, please visit:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm>

## References

[1]RFC 1890: RTP Profile for Audio and Video Conferences with Minimal Control.

<http://www.ietf.org/rfc/rfc1890.txt>

[2]RFC 1889: RTP: A Transport Protocol for Real-Time Applications

<http://www.ietf.org/rfc/rfc1889.txt>

[3]RTP Parameters as defined by IANA: <http://www.iana.org/assignments/rtp-parameters>

[4]Cisco IOS QoS Page: <http://www.cisco.com/warp/public/732/Tech/qos/>

[5]Cisco IOS nBAR Page: <http://www.cisco.com/warp/public/732/Tech/qos/nbar/>

[6]nBAR Documentation: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm>



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 317 7777  
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2002, Cisco Systems, Inc. All rights reserved. CCIP, the Cisco Arrow logo, the Cisco Powered Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratum, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R) ETMG 202822.H/11.02