# Capaciteit- en prestatiebeheer: whitepaper met best practices

## Inhoud



## Inleiding

Hoge netwerkbeschikbaarheid is een bedrijfskritieke vereiste binnen grote ondernemings- en serviceprovidernetwerken. Netwerkmanagers worden geconfronteerd met toenemende uitdagingen bij het bieden van hogere beschikbaarheid, waaronder niet-geplande uitvaltijd, gebrek aan expertise, onvoldoende tools, complexe technologieën, bedrijfsconsolidatie en concurrerende markten. Capaciteit- en prestatiebeheer helpt netwerkmanagers om nieuwe wereldwijde bedrijfsdoelstellingen en consistente netwerkbeschikbaarheid en prestaties te realiseren.

Dit document behandelt de volgende onderwerpen:

- Algemene kwesties inzake capaciteit en prestaties, met inbegrip van de risico's en potentiële capaciteitsproblemen binnen netwerken.
- Capaciteit- en prestatiemanagement best practices, inclusief wat-als-analyses, baselining, trending, uitzonderingsbeheer en QoS-beheer.
- Hoe een strategie voor capaciteitsplanning te ontwikkelen, met inbegrip van

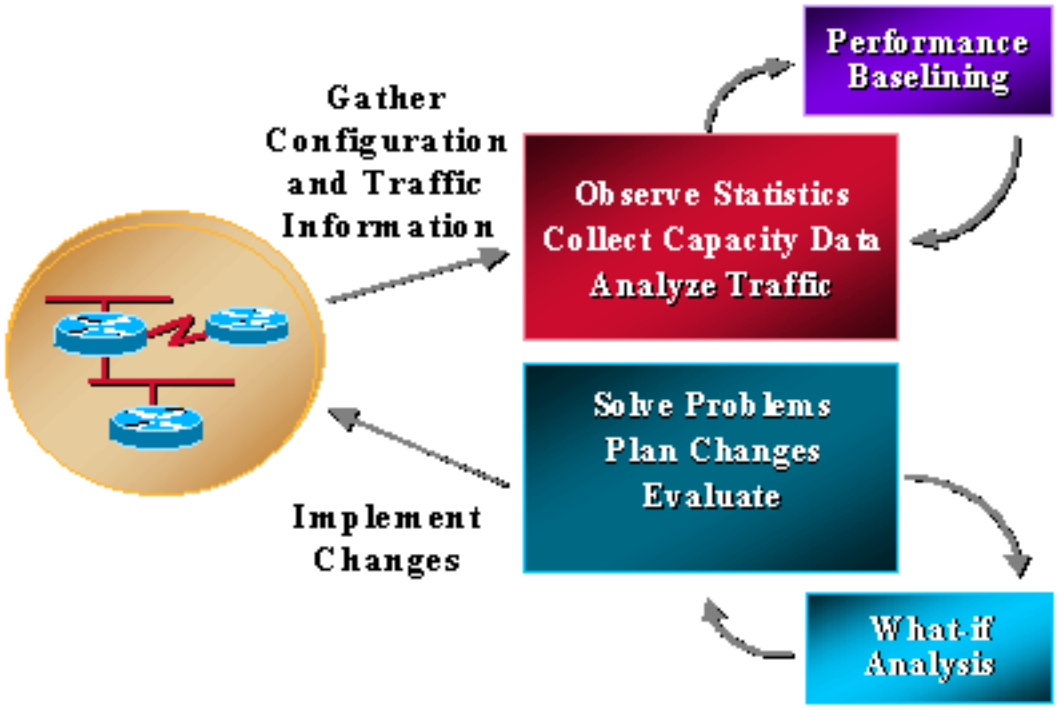
gemeenschappelijke technieken, instrumenten, MIB-variabelen en drempels die bij de capaciteitsplanning worden gebruikt.

## Overzicht van capaciteit- en prestatiebeheer

Capaciteitsplanning is het proces van het bepalen van de netwerkbronnen die nodig zijn om een effect op prestaties of beschikbaarheid van bedrijfskritieke toepassingen te voorkomen. Prestatiebeheer is het beheer van responstijd, consistentie en kwaliteit van netwerkdiensten voor individuele en algemene diensten.

**Opmerking:** prestatieproblemen houden meestal verband met capaciteit. Toepassingen zijn langzamer omdat bandbreedte en gegevens in wachtrijen moeten wachten voordat ze via het netwerk worden verzonden. In spraaktoepassingen hebben problemen zoals vertraging en jitter direct effect op de kwaliteit van de spraakoproep.

De meeste organisaties verzamelen al enkele capaciteitsgerelateerde informatie en werken consequent om problemen op te lossen, wijzigingen te plannen en nieuwe capaciteit en prestatiefuncties te implementeren. Organisaties voeren echter niet routinematig trending en what-if analyses uit. Wat-als de analyse het proces is om het effect van een netwerkverandering te bepalen. Trending is het proces van het presteren bestaan uit basislijnen van netwerkcapaciteit en prestatieproblemen en het herzien van de basislijnen voor netwerktrends om toekomstige upgradevereisten te begrijpen. Het beheer van de capaciteit en van de prestaties zou uitzonderingsbeheer ook moeten omvatten waar de problemen worden geïdentificeerd en opgelost alvorens de gebruikers binnen roepen, en beheer QoS waar de netwerkbeheerders plannen, beheren, en individuele de dienstprestatieskwesties identificeren. De volgende grafiek illustreert de processen van het capaciteit en prestatiesbeheer.




Capaciteit- en prestatiebeheer kent ook beperkingen, die doorgaans te maken hebben met CPU en geheugen. De volgende gebieden kunnen aanleiding geven tot bezorgdheid:

- CPU
- Backplane voor I/O

- Geheugen en buffers
- Interface- en pijpgrootten
- Wachtrijen, vertraging en jitter
- Snelheid en afstand
- Toepassingskenmerken

Enkele verwijzingen naar capaciteitsplanning en prestatiebeheer noemen ook iets dat het "dataplatform" en het "control plane" wordt genoemd. Het gegevensvlak is simpelweg capaciteits- en prestatiekwesties die te maken hebben met de gegevens die het netwerk doorkruisen, terwijl het controlevlak middelen vereist om de juiste functionaliteit van het gegevensvlak te behouden. De functionaliteit van het besturingsplane omvat service-overheadkosten zoals routing, Spanning Tree, interface keep-alives en SNMP-beheer van het apparaat. Deze besturingsplatformvereisten maken gebruik van CPU, geheugen, buffering, wachtrijen en bandbreedte, net zoals het verkeer dat via het netwerk verloopt. Veel van de eisen met betrekking tot het bedieningsvlak zijn ook essentieel voor de algehele functionaliteit van het systeem. Als ze niet over de benodigde bronnen beschikken, mislukt het netwerk.

# CPU

CPU wordt meestal gebruikt door zowel het besturingsplane als het dataplane op elk netwerkapparaat. Bij capaciteits- en prestatiebeheer moet u ervoor zorgen dat het apparaat en het netwerk over voldoende CPU beschikken om te allen tijde te kunnen functioneren. Onvoldoende CPU kan een netwerk vaak samenvouwen omdat ontoereikende resources op één apparaat gevolgen kunnen hebben voor het gehele netwerk. Onvoldoende CPU kan ook de latentie verhogen omdat de gegevens moeten wachten om verwerkt te worden wanneer er geen hardwareschakeling is zonder de belangrijkste CPU.

## Backplane voor I/O

Backplane of I/O verwijst naar de totale hoeveelheid verkeer die een apparaat kan verwerken, meestal beschreven in termen van de grootte van de BUS of backplane mogelijkheid. Onvoldoende backplane resulteert normaal in gevallen pakketten, wat kan leiden tot opnieuw uitzendingen en extra verkeer.

## Geheugen

Geheugen is een andere bron met vereisten voor dataplaat en besturingsplane. Het geheugen is vereist voor informatie zoals het routing van tabellen, ARP-tabellen en andere gegevensstructuren. Wanneer het geheugen van de apparaten is opgebruikt, kunnen bepaalde bewerkingen op het apparaat mislukken. De bediening kan van invloed zijn op regelvlakke processen of dataplatformprocessen, afhankelijk van de situatie. Als de processen van het controlevliegtuig ontbreken, kan het volledige netwerk degraderen. Dit kan bijvoorbeeld gebeuren wanneer er extra geheugen nodig is voor het routeren van convergentie.

## Interface- en pijpgrootten

De interface en de pijpgrootte verwijzen naar de hoeveelheid gegevens die gelijktijdig op om het even welke verbinding kan worden verzonden. Dit wordt vaak ten onrechte de snelheid van een verbinding genoemd, maar de gegevens reizen echt niet met verschillende snelheden van het ene apparaat naar het andere. Siliciumsnelheid en hardwaremogelijkheden helpen de beschikbare bandbreedte te bepalen op basis van de media. Daarnaast kunnen softwaremechanismen

gegevens "verstikken" om te voldoen aan specifieke bandbreedte toewijzingen voor een service. U ziet dit meestal in dienstverlener netwerken voor frame relay of ATM die inherent snelheidscapaciteiten van 1.54kpbs aan 155mbs en hoger hebben. Wanneer er bandbreedtebeperkingen zijn, worden de gegevens een rij gevormd in een verzendrij. Een verzendwachtrij kan verschillende softwaremechanismen hebben om aan gegevens in de wachtrij prioriteit te geven; wanneer er echter gegevens in de wachtrij staan, moet het wachten op bestaande gegevens voordat het de gegevens kan doorsturen naar de interface.

### Wachtrijen, latentie en Jitter

Wachtrijen, vertraging en jitter beïnvloeden ook de prestaties. U kunt de verzendwachtrij zo instellen dat de prestaties op verschillende manieren worden beïnvloed. Bijvoorbeeld, als de wachtrij groot is, dan wachten de gegevens langer. Wanneer wachtrijen klein zijn, worden gegevens verwijderd. Dit wordt taildrop genoemd en is acceptabel voor TCP-applicaties omdat de gegevens opnieuw worden verzonden. Spraak en video presteren echter niet goed met wachtrijval of zelfs aanzienlijke wachtrijlatentie die speciale aandacht vereist voor bandbreedte of pijpgroottes. Wachtrijvertraging kan ook optreden met invoerwachtrijen als het apparaat niet over voldoende resources beschikt om het pakket onmiddellijk door te sturen. Dit kan het gevolg zijn van CPU, geheugen of buffers.

De latentie beschrijft de normale verwerkingstijd vanaf het moment dat deze wordt ontvangen tot het moment dat het pakket wordt doorgestuurd. Normale switches en routers voor moderne gegevens hebben extreem lage latentie (< 1 ms) onder normale omstandigheden zonder bronbeperkingen. Moderne apparaten met digitale signaalprocessors voor het converteren en comprimeren van analoge spraakpakketten kunnen langer duren, zelfs tot 20 ms.

Jitter beschrijft de interpakketkloof voor streaming toepassingen, waaronder spraak en video. Als de pakketten op verschillende tijden met verschillende inter-pakkethiaat timing aankomen, dan is jitter hoog en de stemkwaliteit degradeert. Jitter is vooral een factor van wachttijd.

### Snelheid en afstand

Snelheid en afstand zijn ook een factor in netwerkprestaties. Gegevensnetwerken hebben een consistente snelheid voor het doorsturen van gegevens op basis van de lichtsnelheid. Dit is ongeveer 160 kilometer per milliseconde. Als een organisatie een client-server applicatie internationaal uitvoert, dan kan een corresponderende pakketdoorsturen vertraging verwacht worden. Snelheid en afstand kunnen een geweldige factor zijn voor toepassingsprestaties wanneer toepassingen niet zijn geoptimaliseerd voor netwerkprestaties.

### Toepassingskenmerken

Toepassingskenmerken is het laatste gebied dat de capaciteit en prestaties beïnvloedt. Problemen zoals kleine vensterformaten, applicatieservices en de hoeveelheid gegevens die over het netwerk wordt verzonden in vergelijking met wat er nodig is, kunnen de prestaties van een toepassing in veel omgevingen, met name WAN's, beïnvloeden.

## Best practices voor capaciteit- en prestatiebeheer

In dit gedeelte worden de vijf belangrijkste best practices voor capaciteit- en prestatiebeheer in detail besproken:

## Beheer van serviceniveaus

Beheer op serviceniveau definieert en regelt andere vereiste processen voor capaciteit- en prestatiebeheer. Netwerkmanagers begrijpen dat zij capaciteitsplanning nodig hebben, maar zij worden geconfronteerd met budgetterings- en personeelsbeperkingen die een volledige oplossing verhinderen. Service level management is een beproefde methodologie die helpt bij resourcekwesties door een deliverable te definiëren en een wederzijdse verantwoording te creëren voor een service die gekoppeld is aan dat deliverable. U kunt dit op twee manieren bereiken:

- Maak een overeenkomst op serviceniveau tussen gebruikers en de netwerkorganisatie voor een service die capaciteitsbeheer en prestatiebeheer omvat. De dienst zou rapporten en aanbevelingen omvatten om de dienstkwaliteit te handhaven. De gebruikers moeten echter bereid zijn om de service en eventuele vereiste upgrades te financieren.
- De netwerkorganisatie definieert hun dienst voor capaciteits- en prestatiebeheer en probeert vervolgens per geval financiering voor die dienst en upgrades uit te voeren.

In ieder geval moet de netwerkorganisatie beginnen met het definiëren van een dienst voor capaciteitsplanning en prestatiebeheer die omvat welke aspecten van de dienst die zij momenteel kunnen leveren en wat in de toekomst gepland is. Een complete service zou een wat-als-analyse omvatten voor netwerkwijzigingen en toepassingswijzigingen, baselining en trending voor gedefinieerde prestatievariabelen, uitzonderingsbeheer voor gedefinieerde capaciteits- en prestatievariabelen, en QoS-beheer.

## Network and Application What-if analyse

Voer een netwerk en toepassing wat-als analyse uit om het resultaat van een geplande verandering te bepalen. Zonder een wat-als analyse, nemen de organisaties significante risico's om succes en algemene netwerkbeschikbaarheid te veranderen. In veel gevallen hebben netwerkveranderingen geleid tot een congestieve ineenstorting die vele uren productietijd heeft veroorzaakt. Bovendien is een verbazingwekkende hoeveelheid applicaties mislukt en heeft dit gevolgen voor andere gebruikers en applicaties. Deze mislukkingen blijven in vele netwerkorganisaties, maar zij zijn volledig te voorkomen met een paar tools en enkele extra planningsstappen.

Normaal gesproken hebt u een paar nieuwe processen nodig om een kwaliteit wat-als analyse uit te voeren. De eerste stap is het vaststellen van risiconiveaus voor alle veranderingen en het vereisen van een meer diepgaande "wat als"-analyse voor veranderingen met een hoger risico. Het risiconiveau kan een verplicht veld zijn voor alle wijzigingsaanvragen. Voor veranderingen in het risiconiveau zou dan een welbepaalde "wat als"-analyse van de verandering nodig zijn. Een netwerk wat-als de analyse het effect van netwerkveranderingen op netwerkgebruik en netwerk controle-vlak middelkwesties bepaalt. Een toepassing wat-als analyse het succes van de projecttoepassing, bandbreedtevereisten, en om het even welke kwesties van netwerkmiddelen zou bepalen. De volgende tabellen zijn voorbeelden van toewijzing van risiconiveaus en bijbehorende testvereisten:

| Risiconiveau | Definitie | Aanbevelingen voor wijzigingsplanning |
|---|---|---|
| 1 | • Hoge potentiële impact voor een groot aantal gebruikers (500+) of bedrijfskritieke service als gevolg van nieuwe product, software, topologie of functieintroductie.<br>• De verandering impliceert verwachte netwerk onderaan tijd. | • Bevestig lab van nieuwe oplossing. De validatie van laboratoria omvat gedocumenteerde tests en validatie van oplossingen en een eventuele analyse van de gevolgen voor de bestaande infrastructuur. Wij raden oplossingspilot en aan. Voor nieuwe oplossingen moet een document voor operationele ondersteuning worden ingevuld.<br>• Voer een Cisco NSA-ontwerpbeoordeling uit.<br>• Maak een back-out plan.<br>• Maak een implementatie plan aan.<br>• Wijzig het proces. |
| 2 | • Hoog potentieel effect op een groot aantal gebruikers (500+) of bedrijfskritieke services door een grote toename | • Voer wat-als-analyse uit om de impact op de bestaande omgeving te |

| | | |
|---|---|---|
| | van verkeer of gebruikers, backbonewijzigingen of routeringswijzigingen.<br>• Verandering kan enige uitvaltijd vereisen. | bepalen (moet worden gedaan in lab-omgeving).<br>• Test en bekijk routewijziging en voor functionaliteit.<br>• Maak een back-out plan.<br>• Voer ontwerpbeoordeling uit voor belangrijke routing- of backbonewijzigingen.<br>• Maak een implementatie plan aan.<br>• Wijzig het proces. |
| 3 | • Middelgrote potentiële impact voor kleinere gebruikers of zakelijke service als gevolg van een niet-standaard wijziging.<br>• Omvat nieuw product, software, topologie, toevoeging van eigenschappen voor nieuwe gebruikers, verhoogd verkeer, of niet-standaardtopologie.<br>• Verandering kan enige uitvaltijd vereisen. | • Uitvoeren van engineeringanalyse van nieuwe oplossing (mogelijk moet een laboratoriumvalidatie worden uitgevoerd).<br>• Maak een implementatie plan aan.<br>• Wijzig het proces. |
| 4 | • Vermindert potentiële service- of gebruikersimpact.<br>• Omvat het toevoegen van nieuwe standaardmalplaatjenetwerkmodules, zoals de bouw of server switches/hubs op | • Maak een implementatie plan aan.<br>• Wijzig het proces. |

| | | |
|---|---|---|
| | routers.<br>• Omvat het omhoog brengen van nieuwe WAN-sites of extra bewezen toegangsservices.<br>• Alle veranderingen in risiconiveau 3 zijn technisch bewezen in de productieomgeving.<br>• Verandering kan enige uitvaltijd vereisen. | |
| 5 | • Geen gebruikers- of servicegevolgen.<br>• Omvat het toevoegen van individuele gebruikers aan het netwerk en standaardconfiguratieveranderingen zoals wachtwoord, banner, SNMP, of andere standaardconfiguratieparameters.<br>• Geen uitvaltijd. | • Wijzig proces optioneel. |

Zodra u definieert waar u de wat-als-analyse nodig hebt, kunt u de service definiëren.

U kunt een netwerk uitvoeren wat-als analyse met modelleringshulpmiddelen of met een laboratorium dat de productieomgeving nabootst. De hulpmiddelen van de modellering worden beperkt door hoe goed de toepassing de kwesties van het apparatenmiddel begrijpt en aangezien de meeste netwerkveranderingen nieuwe apparaten zijn, kan de toepassing niet het effect van de verandering begrijpen. De beste methode is om wat vertegenwoordiging van het productienetwerk in een laboratorium te bouwen en de gewenste software, de eigenschap, de hardware, of de configuratie onder lading te testen door verkeergeneratoren te gebruiken. Het lekken van routes (of andere controleinformatie) van het productienetwerk in het laboratorium verbetert ook het laboratoriummilieu. Test extra resourcevereisten met verschillende verkeerstypen, waaronder SNMP, broadcast, multicast, versleuteld of gecomprimeerd verkeer. Met al deze verschillende methodologieën, analyseer de apparatenmiddelvereisten tijdens potentiële spanningssituaties zoals routeconvergentie, verbinding het flappen, en apparatennieuwe begin. Problemen met resourcegebruik zijn onder meer normale capaciteitsresources zoals CPU's, geheugen, backplane gebruik, buffers en wachtrijen.

Nieuwe toepassingen moeten ook een wat-als-analyse uitvoeren om het succes van de toepassing en de bandbreedtevereisten te bepalen. U voert normaal deze analyse in een laboratoriummilieu uit met behulp van een protocolanalysator en een WAN-vertragingssimulator om het effect van afstand te begrijpen. U hebt alleen een pc, hub, WAN-vertragingsapparaat en een laboratoriumrouter nodig die op het productienetwerk zijn aangesloten. U kunt bandbreedte in het laboratorium simuleren door verkeer te verstikken met behulp van generieke traffic shaping of

snelheidsbeperking op de testrouter. De netwerkbeheerder kan samen met de toepassingsgroep werken om inzicht te krijgen in bandbreedtevereisten, vensterproblemen en mogelijke prestatieproblemen voor de toepassing in zowel LAN- als WAN-omgevingen.

Voer een 'wat als'-analyse uit voordat u een zakelijke toepassing implementeert. Als u dit niet doet, geeft de toepassingsgroep de schuld aan het netwerk voor slechte prestaties. Als u op een of andere manier een applicatie kan vereisen wat-als-analyse voor nieuwe implementaties via het veranderingsbeheerproces, kunt u helpen onsuccesvolle implementaties te voorkomen en een beter begrip van plotselinge stijgingen in bandbreedteverbruik voor zowel client-server en batch-vereisten.

## Baselining en trending

Baselining en trending laten netwerkbeheerders toe om netwerkupgrades te plannen en te voltooien voordat een capaciteitsprobleem een netwerk downtime of prestatieproblemen veroorzaakt. Vergelijk het resourcegebruik tijdens opeenvolgende tijdsperioden of deselecteer informatie in de loop van de tijd in een database en laat planners de parameters voor resourcegebruik zien voor het laatste uur, de dag, de week, de maand en het jaar. In beide gevallen moet iemand de informatie wekelijks, tweewekelijks of maandelijks beoordelen. Het probleem met baselining en trending is dat er een overweldigende hoeveelheid informatie nodig is om in grote netwerken te bekijken.

U kunt dit probleem op verschillende manieren oplossen:

- Bouw voldoende capaciteit en switching in de LAN-omgeving zodat capaciteit geen probleem is.
- Verdeel de trendinformatie in groepen en concentreer zich op hoge beschikbaarheid of kritieke gebieden van het netwerk, zoals kritieke WAN-sites of datacenter-LAN's.
- Rapportagemechanismen kunnen gebieden aanwijzen die boven een bepaalde drempel liggen, zodat er speciale aandacht aan kan worden besteed. Als u eerst kritische beschikbaarheidsgebieden implementeert, kunt u de hoeveelheid informatie die voor review vereist is aanzienlijk verminderen.

Bij alle voorgaande methoden moet u de informatie nog regelmatig bekijken. Baselining en trending is een proactieve inspanning en als de organisatie alleen middelen heeft voor reactieve ondersteuning, zullen individuen de rapporten niet lezen.

Veel netwerkbeheeroplossingen bieden informatie en grafieken over de variabelen van de capaciteitsbron. Helaas gebruiken de meeste mensen deze tools alleen voor reactieve ondersteuning van een bestaand probleem. dit gaat voorbij aan het doel van "baselining and trending". Twee tools die effectief informatie over capaciteitstrends voor Cisco-netwerken bieden, zijn het Concord Network Health-product en de INS EnterprisePRO-producten. In veel gevallen gebruiken netwerkorganisaties eenvoudige scripttalen om capaciteitsinformatie te verzamelen. Hieronder staan enkele voorbeeldrapporten die via Script zijn verzameld voor link-gebruik, CPU-gebruik en ping-prestaties. Andere resource variabelen die belangrijk kunnen zijn voor de trend zijn geheugen, wachtrijdiepte, uitzendvolume, buffer, frame relay congestiemelding en backplane gebruik. Raadpleeg deze tabel voor informatie over linkgebruik en CPU-gebruik:

### Koppelingsgebruik

| Bronnen | Adres | Segment | Gemiddeld | Piekgebruik (%) |
|---|---|---|---|---|

| | | | gebruik (%) | |
|---|---|---|---|---|
| JTKR01S2 router | 10.2.6.1 | 128 Kbps | 66.3 | 97.6 |
| JJKR01S0-software | 10.2.6.2 | 128 Kbps | 66.3 | 97.8 |
| FMCR18S4/4 | 10.2.5.1 | 384 Kbps | 51.3 | 109.7 |
| ASR 901S3/1 | 10.2.5.2 | 384 Kbps | 51.1 | 98.4 |

CPU-gebruik

| Bronnen | Stemadres | Gemiddeld gebruik (%) | Piekgebruik (%) |
|---|---|---|---|
| FSTR 901 | 10.28.142.1 | 60.4 | 80 |
| NERT06 | 10.170.2.1 | 47 | 86 |
| NORR01 | 10.73.200.1 | 47 | 99 |
| RTCR01 | 10.49.136.1 | 42 | 98 |

Koppelingsgebruik

| Bronnen | Adres | AvResT (mS) 09-09-98 router | AvResT (mS) 09-09-98 router | AvResT (mS) 09-09-98 router | AvResT (mS) 10-01-98 router |
|---|---|---|---|---|---|
| ADR.01 | 10.190.56.1 | 469.1 | 852.4 | 461.1 | 873.2 |
| ABNR. | 10.190.52.1 | 486.1 | 869.2 | 489.5 | 880.2 |
| APR01 | 10.190.54.1 | 490.7 | 883.4 | 485.2 | 892.5 |
| ASAR01 | 10.196.170.1 | 619.6 | 912.3 | 613.5 | 902.2 |
| ASR 901 router | 10.196.178.1 | 667.7 | 976.4 | 655.5 | 948.6 |
| ASR 901S | | | | | 503.4 |
| AZWRT01 | 10.177.32.1 | 460.1 | | 444.7 | |
| BEJR01 | 10.195.18.1 | 1023.7 | 1064.6 | 1184 | 1021.9 |

## Uitzonderingsbeheer

Uitzonderingsbeheer is een waardevolle methodologie voor het identificeren en oplossen van capaciteits- en prestatieproblemen. Het idee is om een melding te ontvangen van overtredingen van de capaciteit en prestatiedrempels om het probleem onmiddellijk te onderzoeken en op te lossen. Een netwerkbeheerder kan bijvoorbeeld een alarm ontvangen voor een hoge CPU op een router. De netwerkbeheerder kan zich bij de router aanmelden om te bepalen waarom de CPU zo hoog is. Ze kan vervolgens enige corrigerende configuratie uitvoeren die de CPU reduceert of een toegangslijst maken om het verkeer te voorkomen dat het probleem veroorzaakt, vooral als het verkeer niet bedrijfskritisch lijkt.

U kunt uitzonderingsbeheer voor kritischer kwesties vormen vrij eenvoudig met behulp van RMON-configuratieopdrachten op een router of met behulp van geavanceerdere tools zoals Netsys-serviceniveau-beheerder in combinatie met SNMP-, RMON- of NetFlow-gegevens. De meeste netwerkbeheerhulpmiddelen hebben het vermogen om drempels en alarmen op schendingen te plaatsen. Het belangrijkste aspect van het proces van het uitzonderingsbeheer is het verstrekken van dichtbij real-time bericht van de kwestie. Anders verdwijnt het probleem mogelijk voordat iemand heeft gemerkt dat het bericht is ontvangen. Dit kan worden gedaan binnen een NOC als de organisatie consistente monitoring heeft. Anders raden we semafoonmelding aan.

Het volgende configuratievoorbeeld verstrekt stijgend en dalend drempelbericht voor router CPU aan een logboekdossier dat op een verenigbare basis kan worden herzien. U kunt vergelijkbare RMON-opdrachten instellen voor kritische overschrijdingen van de link-gebruiksdrempel of andere SNMP-drempels.

```
rmon event 1 trap CPUtrap description
  "CPU Util >75%"rmon event 2 trap CPUtrap description
  "CPU Util <75%"rmon event 3 trap CPUtrap description
  "CPU Util >90%"rmon event 4 trap CPUtrap description
  "CPU Util <90%"rmon alarm 75 lsystem.56.0 10 absolute rising-threshold
  75 1 falling-threshold 75 2rmon alarm 90 lsystem.56.0 10 absolute rising-threshold
  90 3 falling-threshold 90 4
```

## QoS-beheer

Quality-of-Service beheer omvat het maken en bewaken van specifieke verkeersklassen binnen het netwerk. Een verkeer biedt consistentere prestaties voor specifieke toepassingsgroepen (gedefinieerd binnen verkeersklassen). Traffic shaping-parameters bieden een aanzienlijke flexibiliteit bij het prioriteren en traffic shaping voor specifieke verkeersklassen. Deze functies omvatten mogelijkheden zoals de vastgelegde toegangssnelheid (CAR), de gewogen random vroege detectie (WRED) en op klasse gebaseerde 'fair eighted wachtrij'. Verkeersklassen worden normaal gecreëerd op basis van prestatie-SLA’s voor meer bedrijfskritieke toepassingen en specifieke toepassingsvereisten zoals spraak. Niet-kritisch of niet-zakelijk verkeer zou ook worden gecontroleerd op een manier dat het geen hogere prioritaire toepassingen en diensten kan beïnvloeden.

Het creëren van verkeersklassen vereist een basislijnbegrip van netwerkgebruik, specifieke toepassingsvereisten, en bedrijfsprioriteiten. Toepassingsvereisten omvatten kennis van pakketgrootte, time-outproblemen, jitter-vereisten, burst-vereisten, batch-vereisten en algemene prestatieproblemen. Met deze kennis kunnen netwerkbeheerders traffic-shaping plannen en configuraties maken die consistentere toepassingsprestaties bieden over een groot aantal LAN/WAN-topologieën.

Een organisatie heeft bijvoorbeeld een 10-megabit ATM-verbinding tussen twee grote sites. De link wordt soms verstopt door grote bestandsoverdrachten, wat prestatieverslechtering veroorzaakt voor online transactieverwerking en slechte of onbruikbare spraakkwaliteit.

De organisatie heeft vier verschillende verkeersklassen ingesteld. Voice kreeg de hoogste prioriteit en mocht die prioriteit behouden, zelfs als het doorbrak boven de geschatte hoeveelheid verkeer. De kritieke toepassingsklasse kreeg de volgende hoogste prioriteit maar het werd niet toegestaan om over totale linkgrootte minder te barsten de geschatte vereisten van de stembandbreedte. Als het barst, wordt het verwijderd. Bestandsoverdrachtverkeer kreeg gewoon een lagere prioriteit en al het andere verkeer past ergens in het midden.

De organisatie moet nu QoS-beheer op deze link uitvoeren om te bepalen hoeveel verkeer elke klasse neemt en de prestaties binnen elke klasse te meten. Als de organisatie dit niet doet, kan er voor sommige klassen hongersnood ontstaan of kunnen prestatie-SLA's niet worden gehaald binnen een bepaalde klasse.

Het beheren van QOS-configuraties is nog steeds een moeilijke taak vanwege het gebrek aan tools. Een methode is om de Internet Performance Manager (IPM) van Cisco te gebruiken om ander verkeer te verzenden via de link die in elk van de verkeersklassen valt. U kon prestaties voor elke klasse dan controleren en IPM verstrekt trending, analyse in real time, en hop-door-hop analyse om probleemgebieden aan te wijzen. Anderen kunnen nog steeds vertrouwen op een meer handmatige methode zoals het onderzoeken van de wachtrijen en gedropte pakketten binnen elke verkeersklasse op basis van interfacestatistieken. In sommige organisaties, kunnen deze gegevens via SNMP worden verzameld of in een database voor basislijnen en trending worden geparsed. Er zijn ook tools op de markt die specifieke verkeerstypen over het netwerk sturen om de prestaties voor een bepaalde service of toepassing te bepalen.

## Informatie over verzamel- en rapportagecapaciteit

Het verzamelen en rapporteren van capaciteitsinformatie moet worden gekoppeld aan de drie aanbevolen gebieden van capaciteitsbeheer:

- Wat-als analyse, die rond netwerkverandering centreert en hoe de verandering het milieu beïnvloedt
- Baselining en trending
- Uitzonderingsbeheer

Op elk van deze gebieden een informatieverzamelingsplan ontwikkelen. In het geval van netwerk of toepassing wat-als analyses, hebt u hulpmiddelen nodig om de netwerkomgeving na te bootsen en de invloed van de verandering met betrekking tot potentiële middelkwesties binnen het apparatencontrolevliegtuig of het gegevensvliegtuig te begrijpen. In het geval van baselining en trending, hebt u snapshots nodig voor apparaten en koppelingen die het huidige resourcegebruik tonen. Vervolgens controleert u de gegevens na verloop van tijd om inzicht te krijgen in de potentiële upgradevereisten. Hierdoor kunnen netwerkbeheerders upgrades goed plannen voordat zich problemen met de capaciteit of prestaties voordoen. Wanneer zich problemen voordoen, hebt u uitzonderingsbeheer nodig om de netwerkbeheerders te waarschuwen zodat zij het netwerk kunnen afstemmen of het probleem kunnen oplossen.

Dit proces kan in de volgende stappen worden verdeeld:

1. Bepaal uw behoeften.
2. Definieer een proces.

3. Bepaal capaciteitsgebieden.
4. Definieer de capaciteitsvariabelen.
5. Interpreteer de gegevens.

## Bepaal uw behoeften

Het ontwikkelen van een capaciteit- en prestatiebeheerplan vereist inzicht in de informatie die u nodig hebt en het doel van die informatie. Verdeel het plan in drie vereiste gebieden: elk voor wat-als analyse, baselining/trending, en uitzonderingsbeheer. Ontdek binnen elk van deze gebieden welke middelen en instrumenten beschikbaar zijn en wat nodig is. Veel organisaties falen bij het implementeren van tools omdat ze rekening houden met de technologie en functies van de tools, maar niet met de mensen en expertise die nodig zijn om de tools te beheren. Omvat de vereiste mensen en expertise in uw plan, evenals procesverbeteringen. Deze mensen kunnen systeembeheerders omvatten om de netwerkbeheerstations te beheren, gegevensbankbeheerders om met gegevensbankbeheer te helpen, opgeleide beheerders om de hulpmiddelen te gebruiken en te controleren, en hogere netwerkbeheerders om beleid, drempels, en de vereisten van de informatieverzameling te bepalen.

## Een proces definiëren

U hebt ook een proces nodig om ervoor te zorgen dat de tool met succes en consistent wordt gebruikt. U kunt procesverbeteringen nodig hebben om te definiëren wat netwerkbeheerders moeten doen wanneer er drempelwaardeoverschrijdingen optreden of welk proces moet worden gevolgd voor baselining, trending en upgrade van het netwerk. Zodra u de vereisten en middelen voor succesvolle capaciteitsplanning bepaalt, kunt u de methodologie overwegen. Veel organisaties kiezen ervoor om dit type functionaliteit uit te besteden aan een organisatie voor netwerkservices zoals INS of de expertise intern te ontwikkelen omdat zij de service als een kerncompetentie beschouwen.

## Capaciteitsgebieden definiëren

In het plan voor capaciteitsplanning moeten ook capaciteitsgebieden worden gedefinieerd. Dit zijn gebieden van het netwerk die een gemeenschappelijke capaciteit planningsstrategie kunnen delen: bijvoorbeeld het bedrijfsLAN, WAN-filialen, kritieke WAN-sites en inbeltoegang. Het definiëren van verschillende gebieden is om verschillende redenen nuttig:

- Verschillende gebieden kunnen verschillende drempels hebben. LAN-bandbreedte is bijvoorbeeld veel goedkoper dan WAN-bandbreedte, zodat de gebruiksdrempels lager zouden moeten zijn.
- Voor verschillende gebieden kan het nodig zijn verschillende MIB-variabelen te bewaken. Bijvoorbeeld, zijn de tellers FECN en BECN in Frame Relay kritisch in het begrijpen van frame relay capaciteitsproblemen.
- Het kan moeilijker of tijdrovend zijn om sommige gebieden van het netwerk te bevorderen. Internationale circuits kunnen bijvoorbeeld veel langere doorlooptijd hebben en een corresponderend hoger planningsniveau nodig hebben.

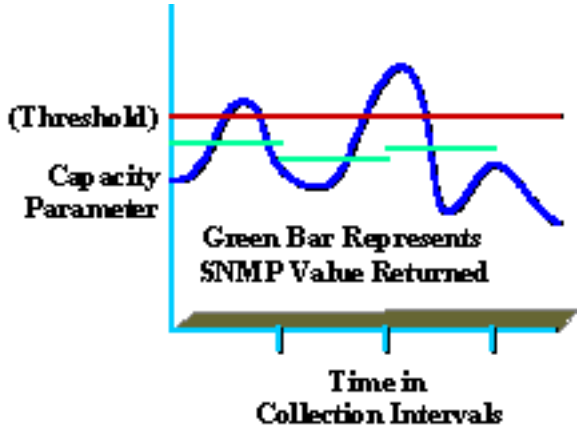
## De capaciteitsvariabelen definiëren

Het volgende belangrijke gebied definieert de variabelen die moeten worden bewaakt en de drempelwaarden die actie vereisen. Het definiëren van de capaciteitsvariabelen hangt aanzienlijk

af van de apparaten en media die binnen het netwerk worden gebruikt. In het algemeen zijn parameters zoals CPU, geheugen en linkgebruik waardevol. Voor specifieke technologieën of vereisten kunnen echter andere gebieden van belang zijn. Deze kunnen rijdiepten, prestaties, frame-relay congestiemelding, backplane gebruik, buffergebruik, netflow-statistieken, uitzendvolume en RMON-gegevens omvatten. Houd in gedachten uw plannen op lange termijn, maar begin met slechts een paar belangrijke gebieden om succes te verzekeren.

### De gegevens interpreteren

Inzicht in de verzamelde gegevens is ook essentieel voor het leveren van een service van hoge kwaliteit. Zo begrijpen veel organisaties bijvoorbeeld de piek- en gemiddelde gebruiksniveaus niet helemaal. Het volgende diagram toont een piek in capaciteitsparameter op basis van een SNMP-verzamelinterval van 5 minuten (weergegeven in groen).




Ook al was de gerapporteerde waarde minder dan de drempelwaarde (weergegeven in rood), toch kunnen er binnen het verzamelinterval nog pieken optreden die boven de drempelwaarde liggen (weergegeven in blauw). Dit is belangrijk omdat tijdens het inzamelingsinterval, de organisatie piekwaarden kan ervaren die prestaties of capaciteit van het netwerk beïnvloeden. Zorg ervoor dat u een betekenisvol verzamelinterval selecteert dat nuttig is en geen overmatige overhead veroorzaakt.

Een ander voorbeeld is het gemiddelde gebruik. Als werknemers slechts van acht tot vijf op kantoor zijn, maar het gemiddelde gebruik is 7x24, kan de informatie misleidend zijn.

## Gerelateerde informatie

- Technische ondersteuning – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.